Current presumptive ranges compared to presumptive ranges in SB 218 January 2006

	First Felony	First Felony (special crimes)	Second Felony	Sex Felony with a prior sex felony	Third+ Felony	Sex Felony with two prior sex felonies	Max
Unclassified Sex Offense	(8 to 12) v< 13: **25 to 30** v>13: **20 to 30**	weapon or serious injury (12 to 6) **25 to 30**	(15 to 20) **30 to 40**	(20 to 30) **35 to 45**	(5 to 35) **40 to 60**	(30 to 40) **99**	99
A Felony Sex Offense	(5 to 8) v<13: **20 to 25** v>13: **15 to 25**	weapon or serious injury (10 to 14) **25 to 35**	(12 to 16) **25 to 35**	(15 to 20) **30 to 40**	(15 to 25) **35 to 50**	(20 to 30) **99**	(30) **99**
B Felony Sex Offense	(2 to 4) **10 to 15** **SFIN CS: 5-15**	n/a	(5 to 8) **10 to 25**	(10 to 14) **15 to 30**	(10 to 14) **20 to 35**	(15 to 20) **99**	(20) **99**
C Felony Sex Offense	(1 to 2) **3 to 12**	n/a	(2 to 5) **8 to 15**	(3 to 6) **12 to 20**	(3 to 6) **15 to 25**	(6 to 10) **99**	(10) **99**

Numbers in parentheses are the current presumptive ranges and maximums

Numbers in **bold** show the new presumptive ranges and new maximums

MYTHS AND FACTS ABOUT "SEX OFFENDERS":
An Initial Response to Senate Bill 218

MYTH: *Sex offenders have a high rate of recidivism and most sex offenders are likely to reoffend.*

FACT: Studies have repeatedly shown that sex offenders have a low rate of recidivism (generally estimated at 5-25%), much lower than the general criminal population. More importantly, studies have shown that recidivist rates vary greatly among the different types of sex offenders and are directly related to specific characteristics of the offender and the offense. First time offenders have consistently been shown to be low-risk.

Sources: "Sex Offender Sentencing: Sentencing Guidelines Commission, 2004," State of Washington Sentencing Commission in response to proposed legislation involving Special Sex Offender Sentencing Alternative (SSOSA) See: http://www.sgc.wa.gov/PUBS/SSOSAReport.pdf; "Assessing Risk Among Sex Offenders In Virginia," Virginia Criminal Sentencing Commission, reported January 2001. See: http://www.vcsc.state.va.us/sex_off_report.pdf; Andrew JR Harris and R. Karl Hanson., "Public Safety and Emergency Preparedness Canada. Sex Offender. Recidivism:. A Simple Question. 2004-03." ww2.psepc-sppcc.gc.ca/publications/corrections/pdf/200403-2_e.pdf; United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, *including statistics showing that the number of substantiated cases of sexual abuse of children declined 40% from 1992 to 2000. Victim-reported sex offenses involving children declined by 56%.*

MYTH: *All sex crimes represent criminal behavior that is grossly deviant and highly dangerous to society*

FACT: Just as the term "sex offender" should not be used as though all persons convicted of sex offenses are the same and equally dangerous, so too should the differences between what qualifies as a "sex offense" be recognized. Under Alaska law, Sexual Assault 2 includes conduct such as fully consensual statutory rape (which can and does include the nineteen year old boyfriend having sex with his fifteen year old girlfriend) and groping (that is, a drunken man touching a woman's breast over her clothing). Currently, a first time offender of Sexual Assault 2 (a person with no prior felony convictions) faces a presumptive term of 2 to 4 years with a maximum of 20 years. Senate Bill 218 seeks to change that to a presumptive term of 10 to 15 years with a maximum of 99 years.

See A.S. 11.41.410-470, defining various levels and culpabilities for the degrees of sexual assault and sexual abuse.

MYTH: *The number of dangerous sex offenders is on the rise.*

FACT: Despite the publicity surrounding certain high profile cases, the rate of sexual assault and child sexual abuse has actually significantly dropped in the last decade. Indeed, a recent study has shown that the rate of sexual assaults per every 1,000 children fell 79% nationwide from 1993 to 2003.

Sources: Analysis by Crimes Against Children Research Center, University of New Hampshire, of date from National Crime Victimization Survey (available at http://www.usatoday.com/news/nation/2005-08-24-sex-crimes-cover_x.htm?POE=NEWISVA); Department of Justice Center for Sex Offender Management Statistics (available at http://www.csom.org/pubs/mythsfacts.html)

MYTH: *There are no wrongfully convicted sex offenders in our system*

FACT: There are almost certainly wrongfully convicted sex offenders in our system. Recent DNA exonerations have demonstrated how faulty eye-witness ideatification can be especially in sex assault cases and non-DNA exonerations involving multiple child victims have shown how frighteningly easy it can sometimes be for young children to falsely accuse someone.

Sources: Samuel [illegible]s et al, *Exonerations in the United States from 1993 to 2003* (available at http://www.mindfully.org/Reform/2004/Prison-Exonerations-Gross19apr04.htm); http://en.wikipedia.org/wiki/False_memory (discussing exonerations involving children's false memories of abuse; *See also* Rob Warden, *The Rape That Wasn't: The First DNA Exoneration in Illinois*, available at http://www.law.northwestern.edu/depts/clinic/wrongful/exonerations/Dotson.htm. (discussing how the first DNA exoneration was a case involving a fabricated accusation of rape against Gary Dotson).

Submitted by Marjorie K. Allard (Marjorie.allard@aya.yale.edu) Cara McNamara (cara_mcnamara@yahoo.com)

THE TRUTH ABOUT
SEXUAL OFFENDER RECIDIVISM

It is widely believed that a person convicted of a sex offense ("a sex-offender") is very likely to commit another sexual offense, and should be viewed as a threat to public safety.

This belief is simply untrue.

The truth is that most sexual offenders never commit another sexual offense after they are released from jail. This has been established by scientific study, over and over. It has been proved right here in Alaska, by our own experts,[1] and world-wide, as well.[2]

75% of the men convicted of a sexual crime will never be convicted of another sexual crime. That's what the data shows.

One of the most prominent researchers to study the question of sexual offender recidivism, Dr. R. Karl Hanson, has published on this subject for the past 20 years, and is widely viewed as one of the world's leading experts on the subject. Dr. Hanson has been consulted, in fact, by the Alaska Department of Corrections itself.

Dr. Hanson, with his colleague Dr. Andrew Harris, recently published a major study of sex offender recidivism, which involved **follow-up studies of more than 4700 men** who had been released from prison after serving time for a sexual offense.[3]

This study established that most sexual offenders do not commit another sexual offense. Three out of four persons who are released from jail after conviction for a sexual offense will not have been charged with any further such offense even after the passage of 15 years.[4]

The truth is that sex offenders are very unlikely to commit another crime. They are much less likely to commit another crime then any other group of criminals. This has been proved in many places, including in Alaska.

It is also important to recognize that some sex offenders are even less likely to recidivate than are others. For example, first-time sexual offenders are significantly less likely to commit any other sexual offense than our offenders with a previous sexual conviction. **80% of first-time sex offenders who are released from prison never commit another sexual offense.**[5]

Other sex offenders who are even less likely to re-offend include those who are over the age of 50 at the time of their release. Nine out of 10 of these older offenders committed no subsequent sexual offense after release. Furthermore, the

longer an offender remains in the community without committing a subsequent offense, the smaller the chance of recidivism is. The greatest risk of recidivism is in the first two years following release.[6]

Factors associated with increased risk for recidivism include 1) male victims, 2) prior sexual offenses, and 3) age under 50 years.[7]

Incest offenders who molest girls recidivate at a significantly lower rate than offenders who target victims outside the family. **Of this group, 85% of those released from prison will not commit another sexual offense within the following 15 years.**[8] Incest offenders who target boys have a higher recidivism rate.[9]

The highest recidivism rates for sexual offenses are for offenders who have more than one sexual conviction. Notably, however, even offenders in this group are not likely to commit another sexual offense. **Over a period of 15 years, 63% of men with more than one conviction for a sexual offense will NOT commit another sexual offense.**[10]

Conclusion: Most of the people who commit a sex offense will never commit another sexual crime. The popular belief that sex offenders are the most dangerous class of criminals is not true. While there are sex offenders who have had many victims, the number of these people in the class as a whole is very small.

---

1 See Mander, Anthony M., Atrops, Martin E., Barnes, Allan R., and Munafo, Roseanne (1996). Sex Offender Treatment Program: Initial recidivism study. This study is available "Sex Offender Recidivism Study" done by the Alaska Department of Corrections, and available through DOC and the UAA Justice Center. Among other things, this study showed that sex offenders as a group are less likely to commit another crime than any other class of criminal.

2 For national statistics, see Becker, J. and Murphy, W., "What We Know and Don't Know about Assessing and Treating Sex Offenders," Psychology, Public Policy and Law 4 (1998).

3 Harris, Andrew J.R. and Hanson, R. Karl (2004). Sex Offender Recidivism: A Simple Question 2004-03. Published by the Solicitor General of Canada, Minister of Public Safety and Emergency Preparedness. I encourage every legislator to review this study. It is available on the Internet at no charge at the followin address:

http://ww2.psepc-sppcc.gc.ca/publications/corrections/pdf/200403-2_e.pdf

4 Hanson & Harris (2004). In another recent study of 9,691 sex offenders, the sexual recidivism rate was only 5.3% after three years. Langan, P.A., Schmitt, E. L., &

Durose, M. R. (2003). Recidivism of sex offenders released from prison in 1994. Bureau of Justice Statistics NCJ 198281. Washington, DC: U.S. Department of Justice. This report is available on the internet at http://www.ojp.usdoj.gov/bjs/abstract/rpr94.htm.

[5] Hanson & Harris (2004), page 7.

[6] Hanson & Harris (2004).

[7] Hanson & Harris (2004), page 11.

[8] Hanson & Harris (2004), page 11.

[9] Hanson & Bussiere (1998).

[10] Hanson and Harris (2004) , page 8.

Sex Crimes Sentencing Comparison									
		1st Felony (Victim Under 13)	1st Felony (Victim 13 or Over)	1st Felony (special: weapon, serious injury)	2nd Felony	2nd Felony with a prior sex felony	3rd Felony	3rd Felony w/2 prior sex felonies	Maximum Penalty
Unclassified Felony (SA 1, SAM 1)	Pre-2003	8	8	10	15	15	25	25	30
	2003	8	8	10	15	20*	25	30*	40
	2005	8-12	8-12	12-16	15-20	20-30*	25-35	30-40*	99
	SB 218	24 - 26	24 - 26	26-30	30-35	35-40*	40-45	99*	99
	CSSB 218	25 - 30	20 - 30	25-35	30-40	35-45*	40-60	99*	99
Class A Sex Offense (Att. SA1, Att. SAM 1)	Pre-2003	5	5	5	10	10	15	15	20
	2003	5	5	10	10	15*	15	20*	30
	2005	5-8	5-8	10-14	12-16	15-20*	15-25	20-30*	30
	SB 218	18-23	18-23	23-26	26-29	29-32*	32-35	99*	99
	CSSB 218	20-25	15-25	25-35	25-35	30-40*	35-50	99*	99
Class B Felony Sex Offense (SA 2, SAM 2, etc)	Pre-2003	0	0	0	4	4	6	6	10
	2003	0	0	0	5	10*	10	15*	20
	2005	2-4	2-4	2-4	5-8	10-14*	10-14	15-20*	20
	SB 218	16-21	16-21	16-21	21-24	24-27*	27-30	99*	99
	CSSB 218	10-15	10-15	10-15	10-25	15-30*	20-35	99*	99
Class C Felony Sex Offense (SA 3, SAM 3, Att. SA 2, Att. SAM 2)	Pre-2003	0	0	0	2	2	3	3	5
	2003	0	0	0	2	3*	3	6*	10
	2005	1-2	1-2	1-2	2-5	3-6*	3-6	6-10*	10
	SB 218	10-15	10-15	10-15	15-18	18-21*	21-24	99*	99
	CSSB 218	3-12	3-12	3-12	8-15	12-20*	15-25	99*	99

*Defendant is Not Eligible for Good Time per AS 33.20.010(a)(3) [2003 Law took away good time if prior sex felony conviction.]

These sentences do not reflect any enhancement for aggravating factors under AS 12.55.155(c).

Pre-2003 Statute: AS 12.55.125(c), (d), (e), and (i)

2003 Statute: §§ 1-5 ch 90 SLA 2003, AS 12.55.125(i)

2005 Statute: §§ 8-13, 32 ch 2 SLA 2005 ("Blakely Bill")

Fax Cover Sheet

From: Anc LIO
907-269-0229

To: Senator Green, Co-Chair
Finance
907-465-2187

Re: SB 218 Written Testimony from

Averic Lerman
Cara Mc Namara
Daniel Bair

25 pages w/ cover sheet
Ruth Keller
269-0111

Andrew J. R. Harris and R. Karl Hanson

Public Safety and Emergency Preparedness Canada

Sex Offender Recidivism: A Simple Question

2004-03

This document is available in French. Ce rapport est disponible en français sous le titre : La récidive sexuelle : d'une simplicité trompeuse.

This document is also available on Public Safety and Emergency Preparedness Canada's Internet site: http://www.psepc-sppcc.gc.ca.

Paper version
Cat. No. PS3-1/2004-3
ISBN 0-662-68211-4

PDF version
Cat. No. PS3-1/2004-3E-PDF
ISBN 0-662-37095-3

Table of Contents

Abstract

This study examines sexual recidivism, as expressed by new charges or convictions for sexual offences, using the data from 10 follow-up studies of adult male sexual offenders (combined sample of 4,724). Results indicated that most sexual offenders do not re-offend sexually, that first-time sexual offenders are significantly less likely to sexually re-offend than those with previous sexual convictions, and that offenders over the age of 50 are less likely to re-offend than younger offenders. In addition, it was found that the longer offenders remained offence-free in the community the less likely they are to re-offend sexually. Data shows that rapists, incest offenders, "girl-victim" child molesters, and "boy-victim" child molesters recidivate at significantly different rates. These results challenge some commonly held beliefs about sexual recidivism and have implications for policies designed to manage the risk posed by convicted sexual offenders.

Introduction

Just about everybody would like to know how often sexual offenders recidivate with another sexual offence. Concerned politicians, an engaged media, and worried parents often assume that the recidivism risk of sexual offenders is extremely high, and routinely ask those working with this population questions such as "all sex offenders do it again don't they?" and "won't they just do it again if you let them out?" Such questions are best answered by appealing to research evidence; first, however, it is important to carefully consider the question being asked.

A Simple Question

The basic question about sexual offender recidivism is usually phrased along the following lines: "what percentage of sexual offenders commit another sexual offence once they've been released from prison?" This question is not as easy to answer as one might believe. First, we must define "recidivism". In some studies, recidivism is defined as a reconviction for a sexual offence (e.g., Hanson, Scott & Steffy, 1995). In other studies, recidivism includes all offenders who were charged with a new sexual offence, whether or not they were convicted (e.g., Song & Lieb, 1995). Including charges along with convictions should, of course, lead to higher estimates of recidivism (Prentky, Lee, Knight & Cerce, 1997). Other studies have used expanded definitions of sexual recidivism that include informal reports to child protection agencies, self-report, violations of conditional release conditions, and simply being questioned by police (e.g., Marshall & Barbaree, 1988). All else being equal, the estimated recidivism rate should increase with each expansion of the definition; the broader the definition, the larger the recidivism estimate should appear. Consequently, it is important to specify the recidivism criteria in any recidivism estimate (e.g., "what percentage of sexual offenders are either charged with, or convicted of, another sexual offence once they've been released from prison?")

Another factor to consider is the length of the follow-up period. As the follow-up period increases, the cumulative number of recidivists can only increase. It is important to remember, however, that an increase in the number of recidivists is not the same as an increase in the yearly rate of recidivism. For all crimes (and almost all behaviours) the likelihood that the behaviour will reappear decreases the longer the person has abstained from that behaviour. The recidivism rate within the first two years after release from prison is much higher than the recidivism rate between years 10 and 12 after release from prison. Consequently, any estimate of sexual re-offending must be "time-defined" or "time limited" (e.g., "over the first five years, post-release from prison, what percentage of sexual offenders are either charged with, or convicted of, another sexual offence?")

A third factor to consider is the diversity among sexual offenders. We know that incest offenders recidivate at a significantly lower rate than offenders who target victims outside the family (Hanson & Bussière, 1998). We also know that child molesters with male victims recidivate at a significantly higher rate than child molesters that only have girl victims (Hanson & Bussière, 1998). By considering the type of sexual offender, our simple question becomes, once again, more complex: (e.g., "over the first five years, post-release from prison, what percentage of child molesters with male victims are either charged with, or convicted of, another sexual offence?")

Many sexual offences are never reported to police; this is the same for all violent offences except murder. Our best estimates of unreported sexual offending come from victimization studies. In a typical study a random sample of people are telephoned and asked if they have been a victim of a crime within the last year. One recent victimization study found that there were approximately half a million sexual

assaults (499,000) committed in Canada in 1999 (Besserer & Trainor, 2000). Although reports to police of violent and sexual crimes were steadily declining in Canada between the years 1993 and 1999; the years 2000 and 2001 saw 1% increases in violent and sexual crimes (Savoie, 2002). Sexual victimization rates based upon victimization surveys appear to have remained basically unchanged across this same time period (Besserer & Trainor, 2000). The Besserer and Trainor (2000) study showed that sexual assault had the highest percentage of incidents that were not reported to police (78%). When respondents were asked why they did not report sexual victimization to the police, 59% of the respondents stated that the "incident was not important enough" to report. Consequently, readers may wonder what counts as a sexual assault.

The Besserer and Trainor (2000) victimization study used a very broad definition of sexual assault. They counted all attempts at forced sexual activity, all unwanted sexual touching, grabbing, kissing, and fondling, as well as threats of sexual assault (Jennifer Tuffs, personal communication, January 15, 2003). Their broad definition undoubtedly included some behaviours that do not conform to the popular image of a sexual offence.

All unwanted sexual advances are wrong, possibly criminal, and have the potential to do psychological harm to the victim. As a society, however, we need to decide whether we wish to count an unwanted touch on the buttocks as an unreported sexual crime. Coming to an agreement on what constitutes a sexual crime will be a difficult task. Setting the bar too low would criminalize social clumsiness and over-state the problem of sexual assault. Setting the bar too high would devalue those victims who, while sustaining no overt signs of trauma, may have truly suffered at the hands of a sexual assailant. A detailed examination of the relationship between observed and undetected sexual offences is beyond the scope of the current paper. Readers should be aware, however, that the answer to the simple question of sexual offence recidivism requires specifying the nature of the offences being considered. In the analyses that follow, recidivism is defined as sexual offences reported to police that are credible and sufficiently serious to justify charges or convictions.

The above review indicates that the simple question is not so simple. Rather than asking "how often do sexual offenders re-offend"; the informed reader would inquire about the recidivism rates of particular types of sexual offenders (e.g., incest offenders versus rapists for example), over a specific time period (e.g., 10 years) using a particular definition of recidivism (e.g., new convictions for a sexual offence). Failure to specify these distinctions can lead to wildly different estimates of the rate of sexual recidivism.

The present study addresses the question of sexual offender recidivism using a large, diverse sample drawn from multiple jurisdictions. The combined sample is sufficiently large (4,724) that it is possible to calculate stable estimates of the observed recidivism rates after five, 10, and 15 years of follow-up for important subgroups of sexual offenders: rapists, girl victim child molesters, boy victim child molesters, incest offenders, those with or without a prior sexual offence, older offenders (age greater than 50 at release) and younger offenders. This study also provides recidivism estimates for sex offenders who have been offence-free in the community for 5, 10, and 15 years.

Method

The Samples

The present sample (N = 4,724) is comprised of 10 individual sub-samples. These sub-samples range in size from 191 offenders to 1,138 offenders and were drawn from the following jurisdictions: Quebec, Ontario, Manitoba, Alberta, California, Washington, Her Majesty's Prison Service (England and Wales), and the Correctional Service of Canada (CSC; 3 data sets). In five of the samples, "conviction for a sexual offence" was used as the recidivism criteria, in another four samples both "charges and convictions for another sexual offence" was used as the recidivism criteria. In one sample (Manitoba), charges, convictions, and additional police information were used as the recidivism criteria. An overview of the samples is presented in Table 1.

All the offenders were released from correctional institutions with the exception of the Manitoba Probation sample and about half of the offenders from the Washington sample, who received community sentences. Racial ethnicity was not recorded for most samples, but given the demographics of the provinces, states and countries from which they were selected, the offenders can be expected to be predominantly white. All offenders were adult males (18 years old or older at time of release). Thirty-seven percent of the offenders were single and 27.9% had previously been sentenced for a sexual offence (9.4% had been sentenced more than once).

Canadian Federal – Pacific Region (CS/RESORS Consulting, 1991; Hanson, Broom & Stephenson, 2004). This study followed sexual offenders released in British Columbia between 1976 and 1992. The original aim of the study was to compare offenders who received mandatory community counselling (n = 401) and those released in earlier years without the benefit of this post-release program (n = 288). Offenders released in the 1983/84 fiscal year (n = 38) were removed from this sample to avoid overlap with the other CSC cohort described below. Recidivism information was coded in 2000 from Royal Canadian Mounted Police (RCMP) records. Charges and convictions for sexual offences were used as the recidivism criteria in this sample.

Canadian Federal Recidivism Study - 1983/1984 Releases (Bonta & Hanson, 1995a; see also Bonta & Hanson, 1995b). This study examined the 316 sexual offenders included in the complete sample of 3,180 federal offenders released by the CSC in the fiscal year 1983/1984. Sexual offenders were defined as those who were released following any sexual conviction. Recidivism information was collected in 1994 using national criminal history records maintained by the RCMP. Conviction for another sexual offence was used as the recidivism criteria in this sample.

Canadian Federal 1991 to 1994 Releases (Motiuk & Brown, 1993; Motiuk & Brown, 1996). This study followed a group of sexual offenders released by CSC between 1991 and 1994. The offenders in this group were those who were reviewed in 1991 (see Motiuk & Porporino, 1993) while they were still incarcerated. Follow-up information was coded in 1994 from RCMP records. Charges and convictions for another sexual offence were used as the recidivism criteria in this sample.

Millbrook Recidivism Study (Hanson, Scott, & Steffy, 1995; Hanson, Steffy, & Gauthier, 1992; Hanson, Steffy, & Gauthier, 1993). This study collected long-term recidivism information (15-30 years) for child molesters released between 1958 and 1974 from Millbrook Correctional Centre, a maximum security provincial correctional facility located in Ontario, Canada. About half of the sample went through a brief treatment program. Recidivism information was coded from RCMP records in 1989 and 1991. Conviction for another sexual offence was used as the recidivism criteria in this sample.

Institut Philippe Pinel (Montreal). (Proulx, Pellerin, McKibben, Aubut & Ouimet, 1997 ; Pellerin et al., 1996). This study focused on sexual offenders treated at a maximum security psychiatric facility between 1978 and 1993. The Institut Philippe Pinel in Montreal provides long term (1-3 years) treatment for sexual offenders referred from both the mental health and correctional systems. Recidivism information

Table 1

Study characteristics.

Sample	Total Sample Size	Age (SD)	Offender type Rape/EX/IN (%)	Sample size for type	Average years of follow-up	Sexual Recid. Rate	Recidivism Criteria
Canadian Federal - Pacific	689	38 (11)	36 / 30 / 33	362	11	24.7	Chgs & Convic
Canadian Federal - 1983/84	316	31 (8.7)	-- / -- / --	0	10	19.7	Convictions
Canadian Federal - 1991/94	241	37 (11)	53 / 19 / 28	208	2	7.1	Chgs & Convic
Millbrook, Ontario	186	33 (10)	00 / 82 / 18	186	23	35.5	Convictions
Institut Philippe Pinel	363	36 (11)	30 / 43 / 27	349	4	16.3	Convictions
Alberta Hospital Edmonton	363	36 (10)	27 / 27 / 46	363	5	5.5	Convictions
SOTEP (California)	1137	38 (8.9)	29 / 40 / 31	1130	5	13.3	Chgs & Convic
HM Prison Service (UK)	529	36 (12)	53 / 32 / 15	325	16	25.7	Convictions
Washington State SSOSA	587	36 (13)	10 / 41 / 49	582	5	7.5	Chgs & Convic
Manitoba Probation	202	35 (12)	26 / 42 / 32	128	2	10.2	Chgs & Convic Plus

Note: EX = Extrafamilial child molesters; IN = Intrafamilial child molesters

was collected in 1994 from RCMP records. Conviction for another sexual offence was used as the recidivism criteria in this sample.

Alberta Hospital Edmonton - Phoenix Program. (Reddon, 1996; see also Studer, Reddon, Roper & Estrada, 1996). The sexual offenders in this study were drawn from those treated at the Phoenix (Alberta Hospital Edmonton) program between 1987 and 1994. The Phoenix program is an eclectic inpatient treatment program that receives many of its referrals from federal correctional facilities. Recidivism information was collected in 1995 using RCMP records. Conviction for another sexual offence was used as the recidivism criteria in this sample.

California's Sex Offender Treatment and Evaluation Project (SOTEP). (Marques & Day, 1996; see also Marques, Day, Nelson & West, 1993; Marques, Nelson, West & Day, 1994). The primary aim of this ongoing study is to examine the efficacy of treatment. The sample used in the current study included sexual offenders randomly assigned to treatment (n = 172), matched volunteer controls, treatment refusers, as well as a general sample of sexual offenders from the California correctional system (total sample of 1,137). Men who had offended only against their biological children were not included. Subjects were admitted to this study between 1985 and 1995; follow-up information was collected in 1995 based on local and national criminal records, as well as local police and probation reports. Charges and convictions for another sexual offence were used as the recidivism criteria in this sample.

Her Majesty's Prison Service (UK). (Thornton, 1997). This study provided a 16 year follow-up of all sexual offenders released from Her Majesty's Prison Service (England and Wales) in 1979 (n = 573). Recidivism information was based on Home Office records collected in 1995. Very few of the offenders in this sample would have received specialised sexual offender treatment. Conviction for another sexual offence was used as the recidivism criteria in this sample.

Washington SSOSA. (Berliner, Schram, Miller & Milloy, 1995; Song & Lieb, 1995). This data set was created to evaluate Washington State's Special Sex Offender Sentencing Alternative (SSOSA), which allows judges to sentence sex offenders to community treatment. To be eligible for SSOSA, offenders must be facing their first felony conviction for sexual crimes other than first or second degree rape. The sample consisted of 287 offenders who received SSOSA and 300 who were statutorily eligible for SSOSA but did not receive it. The majority of the sample was White (85%). Offenders were convicted between January 1985 and June 1986, with follow-up data collected in December, 1990. Charges and convictions for another sexual offence were used as the recidivism criteria in this sample.

Manitoba Probation. (Hanson, 2002). This follow-up study was conducted as an evaluation of a risk scale used by probation officers in Manitoba, Canada. The 202 offenders were consecutive admissions to probation between May, 1997 and February, 1999. Recidivism information was collected in November, 2000, based on RCMP records. Unlike the RCMP records used in the other studies (which included only charges and convictions that went to court), the RCMP records for the Manitoba sample included unresolved charges and cases currently under police investigation.

Analysis

Case specific information (without individual identifiers) from the original 10 data sets were merged for the analysis. Recidivism estimates were computed using survival analysis (e.g., Allison, 1984). This analysis produces the cumulative proportion surviving at the end of a specific time period. These survival percentages were then subtracted from 100 to produce estimates of the recidivism potential at five, ten, and fifteen year intervals. In addition, the standard error of measurement was calculated for these estimates allowing for the calculation of 95% confidence intervals. Confidence intervals of 95% indicate the range within which the observed recidivism percentage should be found "19 times out of 20" or 95% of the time.

Results

Sexual recidivism was measured using the original definitions from the original research reports: 5 data sets used convictions, 4 data sets used new charges (or a new conviction), and one sample used convictions, charges, and additional police information (Manitoba). The five and 10 year recidivism estimates were 17% and 21% for the studies that used only convictions as their recidivism criteria, and 12% and 19% for the studies that used charges and convictions as their recidivism criteria. Given the similarity in the recidivism rates based on convictions alone and charges and convictions, the data was combined to provide overall estimates of sexual recidivism rates. The rates estimated using the combined sample would be closer to the reconviction rate than the re-arrest rate because it appeared that the sources used for the recidivism data contained relatively few charges that did not ultimately result in conviction.

Sexual recidivism rates

Table 2 summarises the recidivism estimates for three distinct time periods, five years, ten years, and fifteen years, for each of the subgroups examined. The overall recidivism rates (14% after 5 years, 20% after 10 years and 24% after 15 years) were similar for rapists (14%, 21% and 24%) and the combined group of child molesters (13%, 18%, and 23%). There were, however, significant differences between the child molesters, with the highest rates observed among the extrafamilial boy-victim child molesters (35% after 15 years) and the lowest observed rates for the incest offenders (13% after 15 years).

Offenders with a prior sexual offence conviction had recidivism rates about double the rate observed for first-time sexual offenders (19% versus 37% after 15 years). Age also had a substantial association with recidivism, with offenders older than age 50 at release reoffending at half the rate of the younger (less than 50) offenders (12% versus 26%, respectively, after 15 years). As expected, those who have remained offence free in the community were at reduced risk for subsequent sexual recidivism. Whereas the average 10 year recidivism rate from time of release was 20%, the 10 year recidivism declined to 12% after five years offence-free and to 9% after 10 years offence-free. The five year recidivism rate for those who had been offence-free for 15 years was 4%. Offence-free was defined as no new sexual or violent non-sexual offence, and no non-violent offences serious enough that they are incarcerated at the end of the follow-up period.

Survival curves

The numbers in Table 2 were drawn from the survival analyses presented in Figures 1 through 6 (see Appendix I). Readers interested in further details of the recidivism rates can use these figures to estimate recidivism rates for different time periods (e.g., 3 years). Each offender is represented on the graph in the top left-hand corner at the time of release (time of sentencing for the community samples). Upon release, none have yet recidivated in the community – hence, 100% have not recidivated at time "0". As time passes (shown on the horizontal axis of the graph) some offenders recidivate and the survival curve descends. In order to know the percentage of offenders who have remained offence-free in the community for 10 years, follow a vertical line from the 10 year mark (on the axis labelled "Time in years") up to the survival curve. Next, go perpendicular from that point on the survival curve to the vertical axis (labelled "percentage of offenders that have not sexually recidivated"). To determine the percentage of offenders that have recidivated, simply subtract the percentage of offenders still in the community from 100.

One factor that should be noted from the graphs is that without exception, the longer offenders remain offence-free in the community the less likely they are to sexually recidivate. The flattening, or plateauing, of the curves over time shows this fact. The steepest part of the curve (the highest risk period) is in the first few years after release.

Table 2

Sexual Recidivism (%) across Time and Samples.

Sub-Group		5 Years	10 Years	15 Years	Shown in Figure #
All sexual offenders		14	20	24	1
Rapists		14	21	24	2
Extended Incest Child Molesters		6	9	13	3
"Girl Victim" Child Molesters		9	13	16	3
"Boy Victim" Child Molesters		23	28	35	3
Offenders without a previous sexual conviction versus those with a previous sexual conviction	Without	10	15	19	4
	With	25	32	37	4
Offenders over age 50 at release versus offenders less than age 50 at release	Over 50	7	11	12	5
	Less than 50	15	21	26	5
Sex Offenders - offence free in the community for Five, Ten, and Fifteen years	5 years	7	12	15	6
	10 years	5	9	‡	6
	15 years	4	‡	‡	6

‡ = Insufficient data to compute reliable estimates

Error of estimation

The data presented in all the graphs and in Table 2 are estimates, and some error is inherent in the estimation process. If the study was repeated with different samples, the numbers would not be exactly the same. One way to appreciate the stability of estimates is to calculate 95% confidence intervals based on the standard error of estimate from survival analysis (see Appendix II). Survival analysis computes standard error of estimate based on the number of recidivists and non-recidivists available at each previous time interval. The 95% confidence intervals indicate the range in which the results are likely to be found, 19 times out of 20, if the study were repeated 20 times.

For example, looking at Appendix II, the five year estimate for the overall sample (14.0%) was based on an initial sample of 4,724 of which 2,492 were followed for at least 5 years. The 95% confidence interval was 12.88% to 15.12%, plus or minus 1.12% from the estimate of 14.0%. With large sample sizes, the confidence intervals are narrow, indicating that subsequent research is likely to find very similar results. Readers should note, however, that confidence intervals expanded with extended follow-up times and when subgroups of offenders were examined. For example, the 15 year estimate for boy-victim child molesters (35.4%), was based upon only 95 observations and had a confidence interval from 29.3% to 40.7% (± 5.7%). Most of the confidence intervals were less than 5%.

Interpretation of recidivism estimates

The recidivism estimates may be applied to the general case or to the individual offender. For example, if you were faced with a group of 100 newly released rapists and you wanted to follow these offenders in the community over time (Looking at Table 2 – Second sub-group – "Rapists") you would expect fourteen (14) of these 100 rapists to reoffend within the first 5 years. In the following 5 years, follow-up years 6 through 10, you would expect a further 7 rapists to reoffend for a total of 21 offenders failing after 10 years. In the following 5 years, follow-up years 10 through 15, you would expect a further 3 rapists to recidivate for a 15-year estimated total of 24 out of 100, or 24% of the sample. It is interesting to note that in each successive 5-year period that the recidivism rate basically halves, from 14% in the first 5 years post-release, to 7% in the second 5-year period, to 3% in the third 5-year period.

You may also estimate the recidivism probabilities of one offender over time. If you have one "typical" rapist, the chance that he will recidivate by the end of the first 5 years would be estimated at 14%, by the end of 10 years at 21%, and by the end of 15 years at 24%. The probability of recidivism for an individual offender will be the same as the observed recidivism rate for the group to which he most closely belongs. The individual's recidivism risk will differ from his group's recidivism rate to the extent that the offender differs from "typical" members of the group (e.g., has committed more or fewer offences than average for that group). It is important to remember that the confidence intervals for the recidivism estimates only apply to the group estimates and not to the individual estimates. In statistical language, the expected mean value for the individual is the same as the group mean, but the variance of the mean is much greater for the individual estimate than for the group estimate.

Discussion

Most sexual offenders do not re-offend sexually over time. This may be the most important finding of this study as this finding is contrary to some strongly held beliefs. After 15 years, 73% of sexual offenders had not been charged with, or convicted of, another sexual offence. The sample was sufficiently large that very strong contradictory evidence is necessary to substantially change these recidivism estimates. Other studies have found similar results. Hanson and Bussière's (1998) quantitative review of recidivism studies found an average recidivism rate of 13.4% after a follow-up period of 4-5 years (n = 23,393). In a recent U.S. study of 9,691 sex offenders. the sexual recidivism rate was only 5.3% after three years (Langan, Schmitt, & Durose, 2003).

Not all sexual offenders, however, were equally likely to reoffend. By using simple, easily observed characteristics, it was possible to differentiate between offenders whose five year recidivism rate was 5%, from those whose recidivism rate was 25%. The factors associated with increased risk were the following: a) male victims, b) prior sexual offences, and c) young age.

Although the number of recidivists increases with extended follow-up, the rate of offending decreases the longer offenders have been offence-free. The five year recidivism rate for new releases of 14% decreased to 4% for individuals who have been offence-free for 15 years. The observed rates underestimate the actual rates because not all sexual offences are detected; nevertheless, the current findings contrast with the popular notion that all sexual offender remain at risk throughout their lifespan.

The observed recidivism rates in the current study are slightly lower than the lifetime sexual recidivism rates estimated by Doren (1998) - 52% for child molesters and 39% for rapists. Doren's estimates were largely based on long-term follow-up of highly selected samples (Hanson et al., 1995; Prentky, et al., 1997); in contrast, the current study used larger and more diverse samples, including many low risk offenders serving community sentences. Doren's (1998) estimates were also based on charges, whereas most of the recidivism data in the current study was based on convictions.

Another difference is that Doren (1998) attempted to generate life-time estimates whereas our estimates extend only to 15 years. We were unable to locate any study that followed a large sample of sexual offenders until they were dead. Very long-term studies are difficult because records go missing, particularly for individuals who have had no recent involvement with the law (Hanson & Nicholaichuk, 2000). Nevertheless, the decreasing rate of offending with age suggests that the rates observed after 15 to 20 years are likely to approximate the rates that would be observed if offenders were followed for the rest of their lives.

When people ask questions about sexual offender recidivism rates, there often is an inherent assumption that the answer is a fixed, knowable rate that will not change. This supposition is unlikely to be true. The rate of sexual re-offence is quite likely to change over time due to social factors and the effectiveness of strategies for managing this population. Most of the offenders in the current study did not receive effective treatment, whereas treatment is currently provided to almost all of the high risk sexual offenders in Canada. Research has found that contemporary cognitive-behavioural treatment is associated with reductions in sexual recidivism rates from 17% to 10% after approximately 5 years of follow-up (Hanson et al., 2002). Furthermore, increased public awareness and concern should reduce the opportunities for sexual offenders to locate potential victims.

Policy implications

Although no finding is ever definitive, the basic findings of the current study are sufficiently reliable to have implications for criminal justice policy. Given that the level of sexual recidivism is lower than commonly believed, discussions of the risk posed by sexual offenders should clearly differentiate between the high public concern about these offences and the relatively low probability of sexual re-offence.

The variation in recidivism rates suggests that not all sex offenders should be treated the same. Within the correctional literature it is well known that the most effective use of correctional resources targets truly high-risk offenders and applies lower levels of resources to lower risk offenders (Andrews & Bonta, 2003). The greater the assessed risk, the higher the levels of intervention and supervision; the lower the assessed risk, the lower the levels of intervention and supervision. Research has even suggested that offenders may actually be made worse by the imposition of higher levels of treatment and supervision than is warranted given their risk level (Andrews & Bonta, 2003). Consequently, blanket policies that treat all sexual offenders as "high risk" waste resources by over-supervising lower risk offenders and risk diverting resources from the truly high-risk offenders who could benefit from increased supervision and human service.

Although the broad risk markers in the current study are useful for estimating recidivism risk, it is possible to improve predictive accuracy by combining such factors into structured risk scales (e.g., Hanson, 1997). The evidence supporting the validity of these risk scales is now sufficient that they should be routinely included in applied risk assessments with sexual offenders (Barbaree, Seto, Langton, Peacock, 2001; Sjöstedt, & Långström, 2001; and reviews by Doren, 2002; Hanson, Morton & Harris, 2003).

Rather than considering all sexual offenders as continuous, lifelong threats, society will be better served when legislation and policies consider the cost/benefit break point after which resources spent tracking and supervising low-risk sexual offenders are better re-directed toward the management of high-risk sexual offenders, crime prevention, and victim services.

Author Note

The views expressed are those of the authors and do not necessarily reflect those of Public Safety and Emergency Preparedness Canada. We would like to thank Jean Proulx, Larry Motiuk, Marylee Stephenson, John Reddon, Lea Studer, Janice Marques, Roxanne Lieb, and Lin Song for access to their original data sets.

Andrew Harris can be reached at Corrections Research, Public Safety and Emergency Preparedness Canada, 340 Laurier Ave., West, Ottawa, K1A 0P8. Andrew.Harris@psepc-sppcc.gc.ca.

References

Allison, P.D. (1984). *Event history analysis : Regression for longitudinal event data.* Beverly Hills, CA: Sage.

Andrews, D. A., & Bonta, J. L. (2003). *The psychology of criminal conduct, Third Edition.* Cincinnati, Ohio: Anderson Publishing.

Barbaree, H. E., Seto, M. C., Langton, C., & Peacock, E. (2001). Evaluating the predictive accuracy of six risk assessment instruments for adult sex offenders. *Criminal Justice and Behavior, 28,* 490-521.

Berliner, L., Schram, D., Miller, L. L., & Milloy, C. D. (1995). A sentencing alternative for sex offenders: A study of decision making and recidivism. *Journal of Interpersonal Violence, 10,* 487-502.

Besserer, S., & Trainor, C. (2000). Criminal victimization in Canada, 1999. *Juristat.* Catalogue no. 85-002-XIE Vol. 20 no. 10. Ottawa: Canadian Centre for Justice Statistics.

Bonta, J., & Hanson, R. K. (1995a). [10-year recidivism of Canadian federal offenders]. Unpublished raw data.

Bonta, J., & Hanson, R. K. (1995b, August). Violent recidivism of men released from prison. Paper presented at the 103rd annual convention of the American Psychological Association: New York.

CS/RESORS Consulting. (1991). *An evaluation of community sex offender programs in the Pacific Region.* Report presented to the Correctional Service of Canada Regional Headquarters (Contract no. 21803-0-A602/01-XSB). Vancouver, B.C.: Author.

Doren, D. M. (2002). *Evaluating Sex Offenders: A manual for civil commitments and beyond.* Sage: Thousand Oaks.

Doren, D. M. (1998). Recidivism base rates, predictions of sex offender recidivism, and the "sexual predator" commitment laws. *Behavioural Sciences and the Law, 16,* 97-114.

Hanson, R. K. (2002). *Evaluation of Manitoba's Secondary Risk Assessment.* Unpublished manuscript. Ottawa: Department of the Solicitor General of Canada.

Hanson, R. K. (1997). *The development of a brief actuarial risk scale for sexual offence recidivism.* (User Report 97-04. Ottawa: Department of the Solicitor General Canada.

Hanson, R. K., Broom, I., & Stephenson, M. (2004). Evaluating community sex offender treatment programs: A 12-year follow-up of 724 offenders. *Canadian Journal of Behavioural Science, 36,* 87-96.

Hanson, R. K., & Bussière, M. T. (1998). Predicting relapse: A meta-analysis of sexual offender recidivism studies. *Journal of Consulting and Clinical Psychology, 66 (2),* 348-362.

Hanson, R. K., Gordon, A., Harris, A. J. R., Marques, J. K., Murphy, W., Quinsey, V., & Seto, M. (2002). The 2001 ATSA report on the effectiveness of treatment for sexual offenders. *Sexual Abuse: A Journal of Research and Treatment, 14 (2),*169-194.

Hanson, R. K., Morton, K. E., & Harris, A. J. R. (2003). Sexual Offender Recidivism Risk: What We Know and What We Need to Know. In R. Prentky, E. Janus, & M. Seto (Eds.), *Understanding and managing sexually coercive behavior* (pp. 154-166). Annals of the New York Academy of Sciences, Vol 989. New York: New York Academy of Sciences.

Hanson, R. K., & Nicholaichuk, T. (2000). A cautionary note regarding Nicholaichuk et al. (2000). *Sexual Abuse: A Journal of Research and Treatment, 12*(4), 289-293.

Hanson, R. K., Scott, H., & Steffy, R. A. (1995). A comparison of child molesters and non-sexual criminals: Risk predictors and long-term recidivism. *Journal of Research in Crime and Delinquency, 32(3),* 325-337.

Hanson, R. K., Steffy, R. A., & Gauthier, R. (1992). *Long-term follow-up of child molesters: Risk prediction and treatment outcome.* (User Report No. 1992-02.) Ottawa: Corrections Branch, Ministry of the Solicitor General of Canada.

Hanson, R. K., Steffy, R. A., & Gauthier, R. (1993). Long-term recidivism of child molesters. *Journal of Consulting and Clinical Psychology, 61*, 646-652.

Langan, P. A., Schmitt, E. L., & Durose, M. R. (2003). Recidivism of sex offenders released from prison in 1984. Bureau of Justice Statistics NCJ 198281. Washington, DC: U.S. Department of Justice.

Marques, J. K., & Day, D. M. (1996). [SOTEP follow-up data for 1995]. Unpublished raw data.

Marques, J. K., Day, D. M., Nelson, C., & West, M. A. (1993). Effects of cognitive-behavioral treatment on sex offenders' recidivism: Preliminary results of a longitudinal study. *Criminal Justice and Behavior, 21*, 28-54.

Marques, J. K., Nelson, C., West, M. A., & Day, D. M. (1994). The relationship between treatment goals and recidivism among child molesters. *Behaviour Research and Therapy, 32*, 577-588.

Marshall, W. L., & Barbaree, H.E. (1988). The long-term evaluation of a behavioural treatment program for child molesters. *Behaviour Research and Therapy, 26(6)*, 499-511.

Motiuk, L. L., & Brown, S. L. (1993). *Survival time until suspension for sex offenders on conditional release.* (Research Report No. R-31). Ottawa, Canada: Correctional Service of Canada.

Motiuk, L. L., & Brown, S. L. (1996). *Factors related to recidivism among released federal sex offenders.* (Research Report No. R-49). Ottawa, Canada: Correctional Service of Canada.

Motiuk, L. L., & Porporino, F. J. (1993). *An examination of sex offender case histories in federal corrections.* (Research Report No. R-30). Ottawa, Canada: Correctional Service of Canada.

Pellerin, B., Proulx, J., Ouimet, M., Paradis, Y., McKibben, A., & Aubut, J. (1996). Étude de la récidive post-traitement chez des agresseurs sexuels judiciarisés. *Criminologie, 29*, 85-108.

Prentky, R. A., Lee, A. F. S., Knight, R. A., & Cerce, D. (1997). Recidivism rates among child molesters and rapists: A methodological analysis. *Law and Human Behavior, 21*, 635-659.

Proulx, J., Pellerin, B., McKibben, A., Aubut, J., & Ouimet, M. (1997). Static and dynamic predictors of recidivism in sexual offenders. *Sexual Abuse, 9*, 7-28.

Reddon, J. R. (1996). [Phoenix Program for Sex Offender Treatment: An evaluation update with recidivism data obtained in September, 1995]. Unpublished raw data.

Savoir, J. (2002). Crime statistics in Canada, 2001. *Juristat*. Catalogue no. 85-002-XPE Vol. 22 no. 6. Ottawa: Canadian Centre for Justice Statistics.

Sjöstedt, G., & Långström, N. (2001). Actuarial assessment of sex offender recidivism risk: A cross validation of the RRASOR and the Static-99 in Sweden. *Law and Human Behaviour, 25*, 629-645.

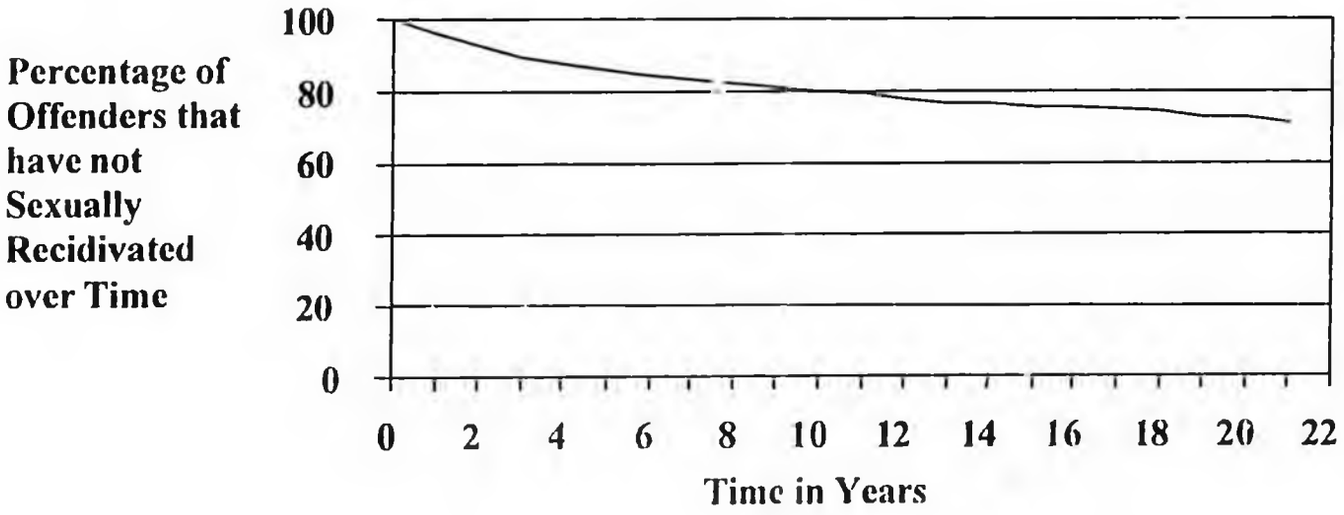
Song, L., & Lieb, R. (1995). *Washington State sex offenders: Overview of recidivism studies.* Olympia, WA: Washington State Institute for Public Policy.

Studer, L. H., Reddon, J. R., Roper, V., & Estrada, L. (1996). Phoenix: An inpatient treatment program for sex offenders. *Journal of Offender Rehabilitation, 23*, 91-97.

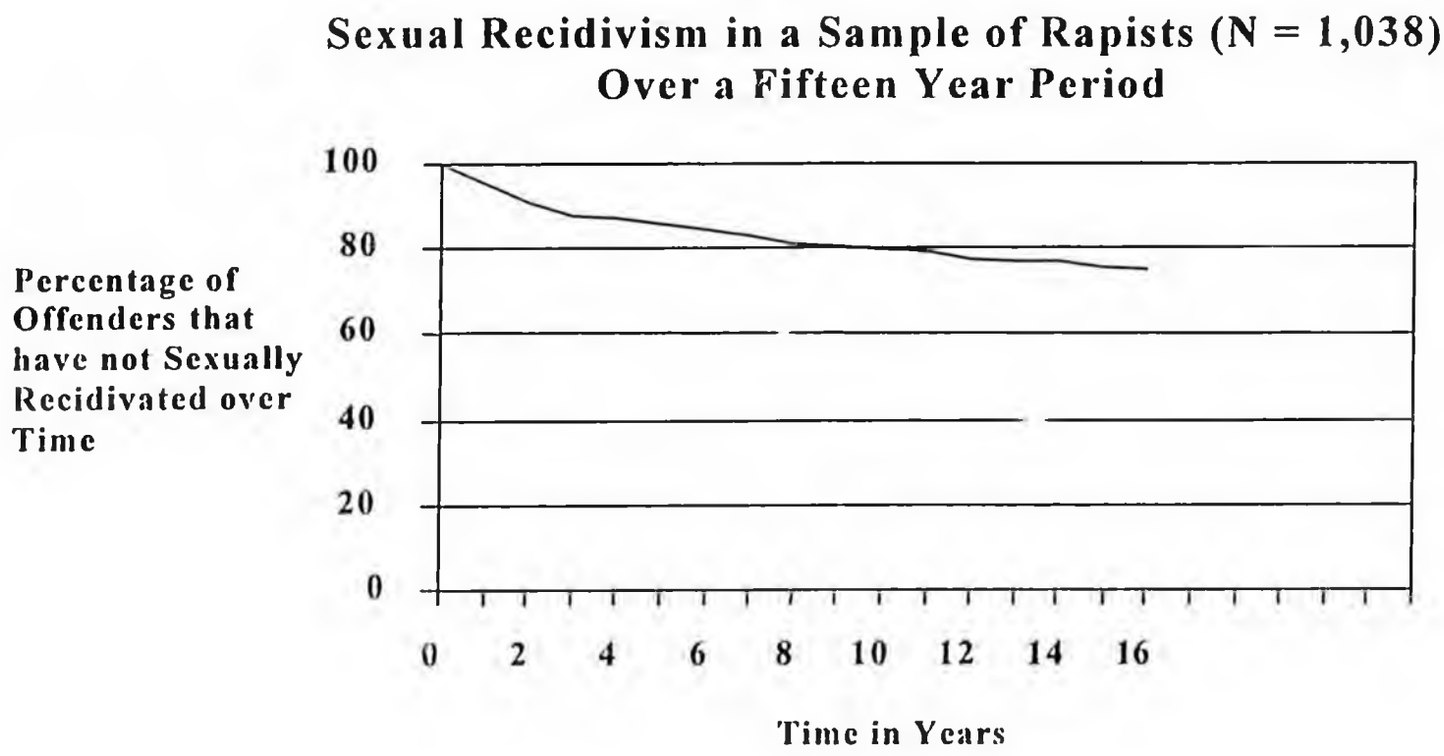
Thornton, D. (1997). [A 16-year follow-up of 563 sexual offenders released from HM Prison Service in 1979.] Unpublished raw data.

Appendix I : Figure 1

Sexual Recidivism in a Sample of Mixed Sexual Offenders (N = 4,724) Over a Twenty Year Period



Appendix I : Figure 2



Presented by:
Averil Lerman
14020 Venus Way
Anchorage, AK 99515

SEXUAL OFFENDER RECIDIVISM:
WHAT IS TRUE AND WHAT IS NOT?

It is widely believed that a person convicted of a sex offense ("a sex-offender") is very likely to commit another sexual offense, and should be viewed as a threat to public safety.

This belief is simply untrue.

The truth is that most sexual offenders never commit another sexual offense after they are released from jail. This has been established by scientific study, over and over. It has been proved right here in Alaska, by our own experts,[1] and world-wide, as well.[2]

75% of the men convicted of a sexual crime will never be convicted of another sexual crime. That's what the data shows.

One of the most prominent researchers to study the question of sexual offender recidivism, Dr. R. Karl Hanson, has published on this subject for the past 20 years, and is widely viewed as one of the world's leading experts on the subject. Dr. Hanson has been consulted, in fact, by the Alaska Department of Corrections itself.

Dr. Hanson, with his colleague Dr. Andrew Harris, recently published a major study of sex offender recidivism, which involved **follow-up studies of more than 4700 men** who had been released from prison after serving time for a sexual offense.[3]

This study established that most sexual offenders do not commit another sexual offense. Three out of four persons who are released from jail after conviction for a sexual offense will not have been charged with any further such offense even after the passage of 15 years.[4]

The truth is that sex offenders are very unlikely to commit another crime. They are much less likely to commit another crime then any other group of criminals. This has been proved in many places, including in Alaska.

It is also important to recognize that some sex offenders are even less likely to recidivate than are others. For example, first-time sexual offenders are significantly less likely to commit any other sexual offense than are offenders with a previous sexual conviction. **80% of first-time sex offenders who are released from prison never commit another sexual offense.**[5]

In addition, the longer an offender remains in the community without committing a subsequent offense, the smaller the chance of recidivism is. The greatest risk of

recidivism is in the first two years following release.[6]

Factors associated with increased risk for recidivism include 1) male victims, 2) prior sexual offenses, and 3) age under 50 years.[7]

Incest offenders who molest girls recidivate at a significantly lower rate than offenders who target victims outside the family. **Of this group, 85% of those released from prison will not commit another sexual offense within the following 15 years.**[8] Incest offenders who target boys have a higher recidivism rate.[9]

The highest recidivism rates for sexual offenses are for offenders who have more than one sexual conviction. Notably, however, even offenders in this group are not likely to commit another sexual offense. **Over a period of 15 years, 63% of men with more than one conviction for a sexual offense will NOT commit another sexual offense.**[10]

Conclusion: Most of the people who commit a sex offense will never commit another sexual crime. The popular belief that sex offenders are the most dangerous class of criminals is not true. While there are sex offenders who have had many victims, the number of these people in the class as a whole is very small.

---

1 See Mander, Anthony M., Atrops, Martin E., Barnes, Allan R., and Munafo, Roseanne (1996). Sex Offender Treatment Program: Initial recidivism study. This study is available "Sex Offender Recidivism Study" done by the Alaska Department of Corrections, and available through DOC and the UAA Justice Center. Among other things, this study showed that sex offenders as a group are less likely to commit another crime than any other class of criminal.

2 For national statistics, see Becker, J. and Murphy, W., "What We Know and Don't Know about Assessing and Treating Sex Offenders," Psychology, Public Policy and Law 4 (1998).

3 Harris, Andrew J.R. and Hanson, R. Karl (2004). Sex Offender Recidivism: A Simple Question 2004-03. Published by the Solicitor General of Canada, Minister of Public Safety and Emergency Preparedness. I encourage every legislator to review this study. It is available on the Internet at no charge at the following address:

http://ww2.psepc-sppcc.gc.ca/publications/corrections/pdf/200403-2_e.pdf

4 Hanson & Harris (2004). In another recent study of 9,691 sex offenders, the sexual recidivism rate was only 5.3% after three years. Langan, P.A., Schmitt, E. L., & Durose, M. R. (2003). Recidivism of sex offenders released from prison in 1994. Bureau of Justice Statistics NCJ 198281. Washington, DC: U.S. Department of Justice. This report is available on the internet at http://www.ojp.usdoj.gov/bjs/abstract/rpr94.htm.

5 Hanson & Harris (2004), page 7.

6 Hanson & Harris (2004).

[7] Hanson & Harris (2004), page 11.

[8] Hanson & Harris (2004), page 11.

[9] Hanson & Bussiere (1998).

[10] Hanson and Harris (2004) , page 8.

MYTHS AND FACTS ABOUT "SEX OFFENDERS":
An Initial Response to Senate Bill 218

MYTH: *Sex offenders have a high rate of recidivism and most sex offenders are likely to reoffend.*

FACT: Studies have repeatedly shown that sex offenders have a low rate of recidivism (generally estimated at 5-25%), much lower than the general criminal population. More importantly, studies have shown that recidivist rates vary greatly among the different types of sex offenders and are directly related to specific characteristics of the offender and the offense. First time offenders have consistently been shown to be low-risk.

Sources: "Sex Offender Sentencing: Sentencing Guidelines Commission, 2004," State of Washington Sentencing Commission in response to proposed legislation involving Special Sex Offender Sentencing Alternative (SSOSA) See: http://www.sgc.wa.gov/PUBS/SSOSAReport.pdf; "Assessing Risk Among Sex Offenders In Virginia," Virginia Criminal Sentencing Commission, reported January 2001. See: http://www.vcsc.state.va.us/sex_off_report.pdf; Andrew JR Harris and R. Karl Hanson., "Public Safety and Emergency Preparedness Canada. Sex Offender. Recidivism:. A Simple Question. 2004-03." ww2.psepc-sppcc.gc.ca/publications/corrections/pdf/200403-2_e.pdf; United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, *including statistics showing that the number of substantiated cases of sexual abuse of children declined 40% from 1992 to 2000. Victim-reported sex offenses involving children declined by 56%.*

MYTH: *All sex crimes represent criminal behavior that is grossly deviant and highly dangerous to society*

FACT: Just as the term "sex offender" should not be used as though all persons convicted of sex offenses are the same and equally dangerous, so too should the differences between what qualifies as a "sex offense" be recognized. Under Alaska law, Sexual Assault 2 includes conduct such as fully consensual statutory rape (which can and does include the nineteen year old boyfriend having sex with his fifteen year old girlfriend) and groping (that is, a drunken man touching a woman's breast over her clothing). Currently, a first time offender of Sexual Assault 2 (a person with no prior felony convictions) faces a presumptive term of 2 to 4 years with a maximum of 20 years. Senate Bill 218 seeks to change that to a presumptive term of 16 to 21 years with a maximum of 99 years.

See A.S. 11.41.410-470, defining various levels and culpabilities for the degrees of sexual assault and sexual abuse.

MYTH: *The number of dangerous sex offenders is on the rise.*

FACT: Despite the publicity surrounding certain high profile cases, the rate of sexual assault and child sexual abuse has actually significantly dropped in the last decade. Indeed, a recent study has shown that the rate of sexual assaults per every 1,000 children fell 79% nationwide from 1993 to 2003.

Sources: Analysis by Crimes Against Children Research Center, University of New Hampshire, of date from National Crime Victimization Survey (available at http://www.usatoday.com/news/nation/2005-08-24-sex-crimes-cover_x.htm?POE=NEWSVA); Department of Justice Center for Sex Offender Management Statistics (available at http://www.csom.org/pubs/mythsfacts.html)

MYTH: *There are no wrongfully convicted sex offenders in our system*

FACT: There are almost certainly wrongfully convicted sex offenders in our system. Recent DNA exonerations have demonstrated how faulty eye-witness identification can be especially in sex assault cases and non-DNA exonerations involving multiple child victims have shown how frighteningly easy it can sometimes be for young children to falsely accuse someone.

Sources: Samuel Gross et al, *Exonerations in the United States from 1993 to 2003* (available at http://www.mindfully.org/Reform/2004/Prison-Exonerations-Gross19apr04.htm); http://en.wikipedia.org/wiki/False_memory (discussing exonerations involving children's false memories of abuse; *See also* Rob Warden, *The Rape That Wasn't: The First DNA Exoneration in Illinois*, available at http://www.law.northwestern.edu/depts/clinic/wrongful/exonerations/Dotson.htm. (discussing how the first DNA exoneration was a case involving a fabricated accusation of rape against Gary Dotson).

Submitted by Marjorie K. Allard (Marjorie.allard@aya.yale.edu) Cara McNamara (cara_mcnamara@yahoo.com)

Sex Crimes Sentencing Comparison								
		1st Felony	1st Felony (special: weapon or serious injury)	2nd Felony	2nd Felony with a prior sex felony	3rd Felony	3rd Felony w/2 prior sex felonies	Maximum Penalty
Unclassified (SA 1, SAM 1)	Pre-2003	8	10	15	15	25	25	30
	2003	8	10	15	20*	25	30*	40
	2005	8-12	12-16	15-20	20-30*	25-35	30-40*	99
	SB 218	24	26-30	30-35	35-40*	40-45	99*	99
Class A Felony Sex Offense (Att. SA1, Att. SAM 1)	Pre-2003	5	5	10	10	15	15	20
	2003	5	10	10	15*	15	20*	30
	2005	5-8	10-14	12-16	15-20*	15-25	20-30*	30
	SB 218	18-23	23-26	26-29	29-32*	32-35	99*	99
Class B Felony Sex Offense (SA 2, SAM 2, etc)	Pre-2003	0	0	4	4	6	6	10
	2003	0	0	5	10*	10	15*	20
	2005	2-4	2-4	5-8	10-14*	10-14	15-20*	20
	SB 218	16-21	16-21	21-24	24-27*	27-30	99*	99
Class C Felony Sex Offense (SA 3, SAM 3, Att. SA 2, Att. SAM 2)	Pre-2003	0	0	2	2	3	3	5
	2003	0	0	2	3*	3	6*	10
	2005	1-2	1-2	2-5	3-6*	3-6	6-10*	10
	SB 218	10-15	10-15	15-18	18-21*	21-24	99*	99

*Defendant is Not Eligible for Good Time per AS 33.20.010(a)(3)
[2003 Changes took away good time if defendant had a prior sex felony conviction.]

These sentences do not reflect any enhancement for aggravating factors under AS 12.55.155(c).

Juneau Office
130 Seward St #209
Juneau, Alaska 99801
Phone: (907) 586-3650
Fax: (907) 463-4493
www.andvsa.org

ANDVSA
Alaska Network on Domestic Violence & Sexual Assault

Sitka Office
PO Box 6631
Sitka, Alaska 99835
Phone: (907) 747-7545
Fax: (907)747-7547

January 30, 2006

The Honorable Senator Con Bunde
State Senate
Alaska State Capitol
Juneau, AK 99801-1182

Dear Senator Bunde:

The Alaska Network on Domestic Violence & Sexual Assault is a coalition of member shelter and community based programs across the state who provide direct services and advocacy for victims of domestic violence and sexual assault. We would like to offer you our support for Senate Bill 218 – An act which requires persons on probation for a sex offense to submit to regular periodic polygraph examinations; increases presumptive ranges for 1st, 2nd, 3rd degree sexual assault or sexual abuse of a minor, incest, indecent exposure in the 1st degree, possession of child pornography, or attempt, conspiracy, or solicitation to commit sexual assault or sexual abuse of a minor in the 2nd degree, unlawful exploitation of a minor or distribution of child pornography; specifies the penalty for failing to report a convicted sex offender.

We appreciate your guidance and leadership in addressing these heinous crimes that wreak havoc on the lives of Alaskans and their children through the generations. It speaks to the fact that Alaska is willing to get tough on these crimes. We cannot merely be informed by the statistic that we are number one in the nation for reported sexual assaults; we must act. It is time we increase sentencing to hold offenders and those who remain silent about them accountable. We fully endorse a containment model of continuous polygraphing of convicted sex offenders.

If I can be of further service to your endeavors, please let me know.

Sincerely,

Peggy Brown
Executive Director

21 January 2006

Mr. Robin W. Swartz
P.O. Box 210094
Auke Bay, Alaska 99821-0094
(907) 523-8143

To the Honorable:

Frank Murkowski	R	Governor
Senator Kim Elton	D	Juneau
Representative Beth Kerttula	D	Juneau
Representative Bruce Weyhrauch	R	Juneau

As the House and Senate debate the issue of Sexual Crimes against our children and punishment for the sex offenders, I would like you to consider the following for offenses against a child under the age of 13 for rape, sodomy, forced sexual acts, molestation and other like crimes.

For the first offense a mandatory sentence of incarceration should be set between an absolute minimum of 25 years to a maximum of 40 years.

In Alaska we had the case of a Wasilla man convicted on five counts of sexually abusing his girlfriend's daughter from the time the girl was 9 until she was 15. In cases that show a child was sexually abused repeatedly, or abused for years, or when multiple children were sexually abused by the same individual; a set of special penalties should be attached to the crime. Even if this is the first time the offender was caught, the repeat offenses are already committed. Second offense penalties should be mandatory with the sentence of 40 years at a minimum to life imposed. We also must assure that the first sex crime does not have to be in Alaska for the 40 year minimum to be imposed.

We have the highest rate of sexual crimes for the nation. We should all be ashamed. We also have a duty to fix this situation and show sexual offenders that they are not welcome in Alaska.

Another way to protect our children is to have a law against convicted sexual predators coming to Alaska without the approval of the state and or registering with the state before coming here. This should include tourists visiting Alaska as well.

Penalties for being present in Alaska while a registered sex offender, or convicted and not registered, from anywhere in the world — without state knowledge and prior approval — should be a minimum of 2 to 5 years at hard labor and expulsion from the state. If the intent was to hide and repeat offend in Alaska — to include possession and trafficking in child pornography — then up to 10 years should be added to any conviction for a sexual offence with the minimum of 5 years imposed — 2 to 5 of those years at hard labor, then expulsion from Alaska. A seizure of all assets should be considered as well

Those presently hiding in the State when this law is passed and haven't committed any other sex crime should have thirty days to register and face expulsion from Alaska, if wanted in another state or country. Those found after the thirty days may expect the whole of the law to be applied regardless of when they came to Alaska.

If a person is convicted of a first offense and sentenced as a first time offender, then later it is discovered that the individual was convicted of a prior sex crime, a 40 year minimum sentence is automatically imposed unless a prosecutor requests a new sentencing hearing to seek more than 40 years. An additional 5 to 10 year add on sentence — with 2 to five years at hard labor — for being a convicted sex offender hiding in Alaska, would also be imposed if the offender was not registered with the state.

I like the proposed polygraph test for released offenders and would suggest internet re-registration with the state once a month as well. I am not opposed to treatment for the offender and hope it helps, but the best answer is to stop the cycle of these sex crimes.

Often offenders were abused children. Many victims go on to a life of drug use and a life of misery. In the case of young girls, many end up prostituting on the streets and often it's to get money for a drug addiction. Young boys have also ended up in a life of prostitution as well. Instead of providing treatment and rehabilitation at state expense for these victims, I propose that all assets in the abusers name be seized to provide for the treatment of the victims. Discretion must be observed and care taken to ensure the seizure of assets does not put the innocent at risk. Then I feel the state should continue treatment after the seized assets are exhausted.

We have the largest state in the union and there are vast areas where someone could hide a child and their activities. Then they could commit their egregious behavior against our children in relative solitude. When I hear of a missing child in Alaska or even a runaway child, I shudder to think what could be happening in our state.

First and most important, the child victim must know that the person or persons who harmed them will never be able to harm them or any other child again during their childhood. Also we must allow a generation of children, from those born at the time of sentencing, to have a childhood free from those individuals. We owe them that.

We will not solve this problem in society. If however; we protect our children, we will start to see generations of children not having to fear shadows, and then I think we will produce a generation enlightened enough to solve this problem. We owe them that chance and until then we must aggressively protect them.

Robin W Swartz

Cc: Sen. Con Bunde, R-Anchorage
Sen. Gretchen Guess, D-Anchorage,
Rep. Mark Neuman, R-Big Lake
Bill O' Reilly Fox News

Constance Hartle

From: Vivian Geroux [stuckupnorth@gmail.com]
Sent: Saturday, January 21, 2006 5:23 PM
To: Sen. Con Bunde
Subject: concerning sex offenders

Dear Mr. Bunde,
I am writing out of extreme concern regarding so many sex offenders out in our neighborhoods. It is frightening to know that a person would commit such crimes--but more frightening to me is that once is not enough to keep them locked up and away from society. Most are let out again and become "repeat offenders" This is unacceptable. I will not pretend I know any laws in specific regarding sex offenders because I do not. I am shocked, however, to know the nature of these crimes against the innocent entail so little punishment. As a greatly concerned parent, a good citezen and a registered voter in your district, I am educating myself on this crucial issue and hope to make a difference by excersising my voting right. It is my hope and prayer that a man in your position would take this matter very seriously and do all that you can to put a stop to these horrific crimes against the innocent. Please do not delay--you have my support in backing stricter laws along with thousands of other people. I thank you for your service in our community and state and for taking the time to read this.

Sincerely, Vivian Geroux

Dist 29

Constance Hartle

From: Dealy Blackshear [blackie_son@yahoo.com]
Sent: Sunday, January 29, 2006 1:20 PM
To: Sen. Con Bunde
Subject: sex offenders

Dear Sen. Bunde,
I am a clinical social worker in Nome. I have been fortunate to work in ten of this region's villages, and come to know many of the people and here and their problems quite well. I applaud the efforts you're making to extinguish the sex abuse problems in the state. You're aim is tru and you are right on target. May I add some thoughts to your quiver.

At Anvil Mountain Correctional Center, prisoners are informally placed in units where other members or their family are kept. Incarceration is a nuisance, not a punishment.

In one case I know of, a man fondled seven little girls at an elementary school where he worked. He was charged with six. He was offered a plea bargain on one count. The little boys in the villages see that old uncle Joe did this thing or that thing to little girls, and came home in 18 months, or 26 months or 90 days. This is no way to train the boys to refrain.

One of my clients was raped by a non-relative in her bedroom repeatedly from the time she was 11 until she was 14. He threatened to kill her family if she told. At age 14, her mother asked finally why she kept coming to sleep with mom and dad at her age. She told. The man was imprisoned. He got out and raped someone else. He was imprisoned again. He got out and raped again. He was imprisoned a 3rd time. This time when he got out, the village prohibited him from coming back. The woman now 25 years old, sought counseling for major depression. She sleeps with a light on and a chest of drawers in front of the door. After ten years the man came home. The now 27 year old woman saw him on the street in her village, and he waved and smiled broadly at her. She moved out of the village. Prison does not help.

We need to change the focus from punishing the offender, to protecting the victim. Please consider the following suggestions:

Any person convicted of a sex crime, may not reside, visit or pass through any village, town or area where the victim of that sex crime lives. That convicted person may not place himself or herself within 25 miles of that victim. If the victim of that crime was a minor at the time of the offense, this distance prohibition is in effect until that victim reaches age 31. If that victim was age 21 or over, that convicted person must maintain that distance for a minimum of ten years. Upon expiration of that distance prohibition, the victim of that sex crime has the right to freedom from intimidation in any manner from that convicted person. Upon proof of intimidation, in addition to any penalties incurred as a result of that intimidation, the distance prohibition shall be extended for 2 years.

Stalking
Any person convicted of stalking the victim of a sex crime, if that convicted person is proven to be family or friend of a person convicted of a sex crime against that victim, or in any way intimidates that victim, that person shall be incarcerated for a minimum of 90 days, and shall forfeit the PFD for one year.

For the person furnishing information leading to the conviction of that person committing the stalking

offense, half the forfeited PFD shall be given as a reward.

Any person convicted of a sex crime, may not possess, borrow, rent, shoot, repair, load, handle, touch or in any other manner use a firearm. For that convicted person that does possess, borrow, rent, shoot, repair, load or in any other manner use handle or touch a firearm, that crime is punishable by two years in prison, per occurrence.

Any person that allows a person convicted of a sex crime access in any manner to a firearm, that person is guilty of a felony, punishable by one year in prison.

Any person aged 21 or over convicted of a sex crime against a minor is guilty of a felony, punishable by a mandatory incarceration minimally not considered completed until the victim of that crime has reached age 21. That convicted person shall forfeit PFD for 20 years.

For the person furnishing information leading to the conviction of that person committing the sex offense, one quarter of the forfeited PFD shall be given as a reward.

Any person convicted of a felony sex crime against a minor regardless of perpetratorâ€™s age, must serve a minimum incarceration of two years, and forfeiture of PFD for 20 years.

For the person furnishing information leading to the conviction of that person committing the sex offense, one quarter of the forfeited PFD shall be given as a reward.

The local communities have difficulty policing sex offenders- every sex offender is someone's son, cousin, uncle, nephew, brother or father. Every woman wants protection from the molester in another family clan, but they do not want their own daddy or son sent away. Victims are routinely ostracized and harrassed for complaining when they are victimized. It will be up to society as a whole (the state) to legislate and protect people that cannot protect themselves.

Thank you for taking the time to read my email. If I can be of any assistance, please don't hesitate to contact me.

Dealy Blackshear LCSW

Constance Hartle

From: robin swartz [robinprime@yahoo.com]
Sent: Sunday, January 22, 2006 9:16 PM
To: Sen. Con Bunde
Subject. Public Opinion Message

Public Opinion
Message 21 Janu...

Senator Bunde
I have written a letter to my Representatives here in Juneau regarding stiffer penalties for sex offenders.
Because you are sponsoring a bill in this area i have also attached a copy for your information and consideration Thank You Robin W Swartz

---

Constance Hartle

From: April Warwick [analw2@uaa.alaska.edu]
Sent: Thursday, January 26, 2006 12:46 PM
To: Sen. Con Bunde
Subject: Wanting to help

Hello Con Bunde:

My name is April Warwick. In the Anchorage Daily News, I saw an article stating your plans to create stricter laws for individuals who sexually abuse children. I'd like to encourage you to continue your work, it's well needed. Personally, I think offenders of children should get mandatory life sentences. This is an issue I want to work on more in the future and I'm looking for ways I could be helpful. Is there anything I could do to help you? Are there any groups working on this issue that I could work with?

April Warwick
5716 Kennyhill Drive
Anchorage, AK 99504
(907) 338-7777 (hm)
(907) 264-6255 (wk)

SENATE COMMITTEE REPORT
First Committee of Referral

DATE: 1/9/06

FURTHER: (Finance)

Date of 5-Day Notice: 1/12/06
(in accordance with Uniform Rule 23)

DATE TURNED IN TO OFFICE: 1/24/06

Judiciary Committee considered SENATE BILL NO. 218

SB 218 CRIMINAL SENTENCING AND POLYGRAPHS

"An Act relating to periodic polygraph examinations for sex offenders released on probation or parole and to sentencing for sex offenders and habitual criminals."

and recommends:

[✓] be replaced with _____ CS SB 218 (JUD)

[ ] adopt previous _____ CS _____ (_____)

[ ] attached amendment(s)

[ ] adopt Letter of Intent by _____ Committee

[ ] further referral to _____ Committee

CS Senate Bill:
[ ] Same Title
[✓] New Title

SCS House Bill:
[ ] Same Title
[ ] Technical Title Change
[ ] New Title w/ SCR # _____

NEW FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#
DPS	1/18/06			✓	1
ADM.	1/18/06		✓		2
ADM	1/17/06		✓		3
LAW	1/18/06		✓		4

PREVIOUS FISCAL NOTE(S):

Department	Date	Fiscal	Indet.	Zero	FN#

[ ] **APPROPRIATION - no fiscal note**

	SIGNATURES AND RECOMMENDATIONS:	DO PASS	DO NOT PASS	NO REC	AMEND
French				X	
Guess		✓			
Therriault					✓
Huggins					✓
Seekins	CHAIR:			X	

SB

222

SFIN

FILE

SB 222

was referred to the Senate Finance Committee

Hearing(s) were held

The bill did not move from Committee

Alaska State Legislature

SENATOR
GENE THERRIAULT
Mailing Address:
1904, Cushman, Suite 101
Fairbanks, Alaska 99701
(907) 488-0857
Fax: (907) 488-1271

While in session:
State Capitol
Juneau, Alaska
99801-1182
(907) 465-4797
Fax: (907) 465-3884
Senate District F

Senate

Sponsor Statement

Senate Bill 222

Consumer Privacy Protection Act

I have introduced Senate Bill 222 to address the ever-increasing risks to consumers as their personal information is collected, distributed, and discarded by both private sector and government entities.

Senate Bill 222 tightens security measures pertaining to personal information as well as timelines to better notify consumers of potential problems so they may take remedial action as quickly as possible.

Consumers have every right to expect their private records are well protected and that their personal credit information is accurate. They also must have reasonable recourse when potentially damaging inaccurate information is made public including ample opportunities for redress and restitution in a timely manner.

In summary, Senate Bill 222 requires parties that handle and distribute sensitive consumer information to be accountable and responsible in those activities.

THE
FOLLOWING
DOCUMENT(S)
ARE
POOR
ORIGINAL
COPIES

National Card Coalition

Security Breach

Enacted Legislation

February 20, 2006

Post Office Box 3188
Laurel, MD 20709-3188
(202) 783-7766 phone

Security Breach Enacted Legislation

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice - OCC Bulletin 2005-13 **Breach Provisions Effective:** 03/29/05 **Enforcement:** Functional regulator **Penalties:** Refer to GLBA, 15 U.S.C. 6801, Section 501(b) and Interagency Guidelines Establishing Information Security Standards (Security Guidelines) **Summary:** Pursuant to the Gramm-Leach-Bliley Act, the federal banking agencies issued joint proposed guidance regarding security breaches in 2003 but did not finalize that guidance until March 29, 2005 when they issued the final Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. This Guidance interprets Section 501(b) of GLBA and Interagency Guidelines Establishing Information Security Standards (the "Security Guidelines") and describes response programs, including customer notification procedures, that financial institutions should develop and implement to address unauthorized access to or use of customer info. that could result in substantial harm or inconvenience to customer. **Preemption of state law** not addressed http://www.occ.treas.gov/ftp/bulletin/2005-13.doc	Financial institutions regulated by federal banking agencies. Every financial institution should develop and implement response program designed to address incidents of unauthorized access to customer info. maintained by institution or its service provider. Final guidance provides each financial institution with greater flexibility to design risk-based response program tailored to size, complexity and nature of its operations.	**Trigger** Reasonable **investigation** to promptly determine likelihood that sensitive customer info. has been or will be misused. Notice required if determination that misuse has occurred or is reasonably possible. **Method** No specific method for providing notice is required - any manner designed to ensure that a customer can reasonably be expected to receive it (i.e., telephone, mail, email) ***Guidance specifies notice content.*** **Timing** As soon as possible.	Customer name, address or telephone # in conjunction with any one or more data elements: • SS # • State DL # • account # • credit or debit card # • personal ID # or code that would permit access to a customer's account • any combination of components of customer info. that would allow someone to log onto or access customer's account, such as user name and password or password and account number. Does not exclude info. that is publicly available.	Delay for law enforcement **investigation.**	**3rd Party Notice** An institution's contract with its service provider should require service provider to take appropriate actions to address incidents of unauthorized access to financial institution's customer info., including notification to institution as soon as possible of any such incident, to enable institution to expeditiously implement its response program. Encouraged but not required to notify CRAs and federal regulators.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Arkansas S 1167 **Sponsor:** Capps (D) **Introduced:** 03/07/05 **Enacted:** 03/31/05 **Act/Chapter Number:** 1526 **Breach Provisions Effective:** 08/12/05 **Enforcement:** AG action; AG criminal action for knowing and willful violation, private right of action. **Penalties:** Class A misdemeanor, punishable by up to 1 year in prison and fine of up to $1K for knowing and willful violation; restitution; injunction; enjoinment; civil penalties up to $10K per violation; actual damages and reasonable attorney's fees. **Summary:** Relates to the protection of personal info. and the disclosure of security breaches of computerized data that includes personal info., that was reasonably believed to have been acquired by an unauthorized person, in an expedient manner using various specified methods. **State agency** security breaches included in act via "business" definition. **Identity theft measure** also includes provisions for destruction of customer records containing personal info. http://www.arkleg.state.ar.us/ftproot/acts/2005/public/act1526.pdf	Person or business that acquires, owns or licenses computerized data that includes personal info. **Security breach** defined as unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal info. maintained by a person or business. Does not include good faith acquisition of personal info. by employee/agent of person/ business for legitimate purposes of person/business if personal info. is not otherwise used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info. to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data element is not encrypted or redacted. • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password • medical info. Does ***not*** exclude info. that is publicly available.	Delay for law enforcement **investigation.** Notice not required if reasonable **investigation** determines no reasonable likelihood of harm to customers. **Safe harbor** for providing notice pursuant to an internal info. security policy.	3rd Party Notice Person doing business maintaining computerized data including personal info. not owned must immediately notify information owner/licensee of any system breach immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**Exempts from act's security breach subchapter** businesses regulated by state or federal law that provides greater protection to personal info. and at least as thorough disclosure requirements for breach.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
California S 1386 **Sponsor:** Peace(D) **Introduced:** 2/12/02 **Enacted:** 09/26/02 **Act/Chapter Number:** 915 **Breach Provisions Effective:** 07/01/03 **Enforcement:** Private right of action. **Penalties:** Damages; civil penalty up to $3K per violation; enjoinment. **Summary:** Requires a State agency, or a person or business that conducts business in the State that owns or licenses computerized data that includes personal info. to disclose in specified ways, any breach of the security of the data to any State resident whose unencrypted personal info. was or may have been acquired by an unauthorized person. **Preempts** all rules, regulations, codes, statutes, or ordinances or all cities, counties, cities and counties, municipalities, and other local agencies. **State agency** security breaches addressed in Section 2 of act. http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html	Person or business that conducts business in CA and owns or licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by person/business. Good faith acquisition of personal info. by employee or agent of person/business for purposes of person/business is not breach of system security, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person doing business maintaining computerized data including personal info. not owned must immediately notify information owner/licensee of any system breach immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Connecticut S 650 **Sponsor:** Looney (D) **Introduced:** 1/21/05 **Enacted:** 06/24/05 **Act/Chapter Number:** 05-148 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; consumer civil and class action. **Penalties:** Temporary/permanent restraining orders; enjoinment; civil penalties of 5-25K per violation; actual damages; costs and reasonable attorneys' fees. **Summary:** Requires businesses to inform the public if there has been a security breach. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions for security freezes and other credit report protections. http://www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm	Person who conducts business in CT and owns, licenses or maintains computerized data that includes personal info. **Security breach** defined as unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal info. when access to personal info. has not been secured by encryption or by any other method or technology that renders personal info. unreadable or unusable.	**Trigger** Personal info. was or is reasonably believed to have been accessed by an unauthorized person. **Method** Written, electronic or telephonic. **Timing** Without unreasonable delay consistent with law enforcement needs and other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written electronic or telephonic notice **Substitute Method** Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records or widely distributed media	Delay for law enforcement **investigation**. Notice is not required if, after an appropriate **investigation** and consultation with law enforcement, it can be reasonably determined that the breach will not likely result in harm to any individual whose info. was acquired and accessed. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data including personal info. not owned shall notify info. owner/ licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been accessed by unauthorized person.	**In compliance with chapter's security breach notification section** pursuant to rules, regulations, procedures or guidelines established by person's primary or functional federal regulator, provided notice is made in accordance with established security breach procedures if system security breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Delaware H 116 **Sponsor:** Gilligan **Introduced:** 4/1405 **Enacted:** 06/28/05 **Act/Chapter Number:** 61 **Breach Provisions Effective:** 06/28/05 **Enforcement:** AG action. **Penalties:** Direct economic damages. **Summary:** Requires individual or commercial entity that conducts business in Delaware and that owns/licenses computerized data that includes personal info. about resident of Delaware, when it becomes aware of system security breach, conduct in good faith reasonable and prompt investigation to determine likelihood that personal info. has been or will be misused. Notice shall be given as soon as possible to affected Delaware residents if investigation determines that misuse of info. has occurred or is reasonably likely to occur. **State agency** security breaches included in act via "commercial entity" definition. http://www.delcode.state.de.us/title6/c012b/index.htm#TopOfPage	Individual or commercial entity that conducts business in DE and owns/licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition of unencrypted computerized data that compromises security, confidentiality, or integrity of personal info. maintained by individual or commercial entity. Good faith acquisition of personal info. by an employee/agent of individual or commercial entity for purposes of individual or commercial entity is not a system security breach, provided that personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Misuse of personal info. has occurred or is reasonably likely to occur. **Method** Written, electronic or telephonic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs and other necessary measures. **Substitute Trigger** • cost exceeds $75K, or • affects more than 100K people, or • not enough info to provide written, electronic or telephonic notice **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements, when either the name or the data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Individual or commercial entity that maintains computerized data that includes personal info. that individual or commercial entity does not own or license shall give notice to and cooperate with owner/licensee of info. regarding any system security breach immediately following discovery of such, if misuse of personal info. occurred or is reasonably likely to occur. Cooperation includes sharing with owner or licensee info. relevant to breach.	**In compliance with chapter** if regulated by state or federal law, maintains security breach procedures pursuant to laws, rules, regulations, guidance or guidelines established by primary or functional state/federal regulator; and notifies affected residents as per maintained security breach procedures when breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Florida H 481 **Sponsor:** Waters (R) **Introduced:** 03/08/05 **Enacted:** 06/14/05 **Act/Chapter Number:** 2005-229 **Breach Provisions Effective:** 07/01/05 **Enforcement:** Dept. of Legal Affairs (AG) action. **Penalties:** Administrative fine per breach not to exceed $500K ($1K /day each day breach goes undisclosed up to 30 days, thereafter $50K for each 30-day period or portion thereof up to 180 days; if notification not made within 180 days, administrative fine up to $500K); failure to document "notice not required" determination liable for administrative fine up to $50K. **Summary:** Relates to undisclosed computer data security breaches. **State agency** security breaches included via "person" definition.. agency breaches of personal info. in custody of gov. agency or subdivision exempt from adminstrative sanctions of act unless governmental agency or subdivision has entered into contract with contractor or 3rd-party administrator to provide governmental services, at which point contractor or 3rd-party administrator is responsible. **Identity theft measure** also includes other non-business identity theft related provisions. http://election.dos.state.fl.us/laws/05laws/ch_2005-229.pdf	Person who conducts business in FL and maintains computerized data that includes personal info. **Security breach** defined as unlawful and unauthorized acquisition of computerized data that materially compromises security, confidentiality, or integrity of personal info. maintained by person. Good faith acquisition of personal info. by employee/ agent of person is not security system breach, provided info. is not used for purpose unrelated to business or subject to further unauthorized use.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by unauthorized person. **Method** Written or electronic notice. **Timing** Notice must be made ***no later than 45 days*** from determination of breach unless otherwise provided, including law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	**Individual's first** name, first initial and last name, or any middle name and last name, in combination with any one or more of following data elements when data elements are not encrypted: • SS # • State DL or ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records or widely distributed media	Delay for law enforcement **investigation**. Notice not required if determintion is made, after investigation or consultation with law enforcement, that breach has not or will not likely result in harm to individuals. Determination must be documented in writing and maintained for 5 years. Safe harbor for providing method of notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person who maintains computerized data including personal info. on behalf of another business entity shall disclose to business entity for which info. is maintained any system security breach as soon as practicable, **but no later than 10 days** following determination, if personal info was or is reasonably believed to have been acquired by unauthorized person (see statute for further info. regarding notification responsibility). If notice required to more than 1,000 persons at a time, then also must notify CRA of notice timing, distribution and content.	**In compliance with chapter's security breach notification section** provided notice is made in accordance with person's policies or rules, regulations, procedures or guidelines established by person's primary or functional federal regulator if system security breach occurs.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Georgia S 230 **Sponsor:** Hamrick (R) **Introduced:** 02/22/05 **Enacted:** 05/05/05 **Act/Chapter Number:** 163 **Breach Provisions Effective:** 05/05/05 **Enforcement:** Act is silent. **Penalties:** Act is silent. **Summary:** Requires info. brokers give notice to consumers of certain security breaches. **State agency** security breaches not specifically addressed in act; governmental agencies whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes are exempt from "info. broker" definition. http://www.legis.ga.gov/legis/2005_06/versions/sb230_AP_12.htm	**Info. broker** that maintains computerized data including personal info. Info. broker defined as person or entity who for monetary fees/dues collects, assembles, evaluates, compiles, reports, transmits, transfers or communicates info. concerning individuals for primary purpose of furnishing to nonaffiliated 3rd parties. **Security breach** defined as unauthorized acquisition of individual's computerized data compromising security, confidentiality, or integrity of individual's personal info. maintained by info. broker. Good faith acquisition of personal info. by info. broker employee/ agent for info. broker purposes is not system security breach, provided personal info. is not used/subject to unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic notice. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info. to provide written or electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one/more of following data elements when either name or data elements are not encrypted or redacted: • SS # • State DL # or ID# • account, credit card or debit card # if usable w/out additional identifying info., access codes or passwords • account passwords or personal ID #s or other access codes • any above items when not in connection with individual's first name or first initial and last name, if info. compromised would be sufficient to perform or attempt to perform ID theft. Excludes info. publicly available from federal, state or local government records	Delay for law enforcement **Investigation.** Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data on behalf of info. broker, including personal info. not owned, shall notify info. broker of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been, acquired by unauthorized person. If notice required for more than 10,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Illinois H 1633 **Sponsor:** Madigan (D) **Introduced:** 02/14/05 **Enacted:** 06/16/05 **Act/Chapter Number:** 94-0036 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; private right of action. **Penalties:** Enjoinment; injunction, restitution; revocation; forfeiture or suspension of any license, charter, franchise, certificate or other evidence of authority of to do business in state; civil fine up to $50K per violation; additional fine up to $10K per violation against person over 65 years old; actual economic damages (punitive damages, injunctive relief, and/or reasonable attorney's fees and costs). **Summary:** Provides that any data collector shall notify a resident if there has been a breach of the security of the system data, without regard for whether the data has been accessed for legal or illegal purposes. **State agency** security breaches included in act via "data collector" definition. http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036&print=true	Any data collector that owns/licenses personal info. ...cerning IL ...dent. Data ...ector definition includes financial institutions. Security breach defined as unauthorized acquisition of computerized data compromising security, confidentiality, or integrity of personal info. maintained by data collector. Does not include good faith acquisition of personal info. by data collector employee/ agent for data collector's legitimate purpose, provided personal info. is not used for purpose unrelated to data collector's business or subject to further unauthorized disclosure.	Trigger **Discovery or notification of breach alone triggers notice requirement; no further standard articulated.** Method Written or electronic notice. Timing Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. Substitute Trigger • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. Substitute Method Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted or redacted • SS # • State DL# or ID# • account, credit card or debit card #, or account or credit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Does NOT allow delay for law enforcement investigation. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice Data collector that maintains computerized data including personal info. not owned shall notify information owner or licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Louisiana S 205 **Sponsor:** Duplessis (D) **Introduced:** 04/15/05 **Enacted:** 07/12/05 **Act/Chapter Number:** 499 **Breach Provisions Effective:** 01/01/06 **Enforcement:** Private right of action. **Penalties:** Actual damages, based on rules to be promulgated by AG. **Summary:** Database Security Breach Notification Law. **State agency** security breaches included. http://www.legis.state.la.us/billdata/streamdocument.asp?did=320093	Person that conducts business in LA or owns or licenses computerized data that includes personal info. **Security** breach defined as compromise of security, confidentiality, or integrity of computerized data that results in, or is reasonable basis to conclude has resulted in, unauthorized acquisition of and access to personal info. maintained by agency/person. **Good faith** acquisition of personal info. by agency/person employee/ agent for purposes of agency/person is not system security breach, provided that personal info is not used for, or subject to, unauthorized disclosure.	**Trigger** Unencrypted or not redacted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted or redacted: • SS # • State DL # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **Investigation.** Notice not required if, after reasonable **investigation**, person or business determines that no reasonable likelihood of harm to customers. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Agency/person that maintains computerized data which includes personal info. not owned shall notify information owner/licensee of any security breach of data following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**In compliance with chapter** for financial institutions subject to and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Maine H 1180a **Sponsor:** Pelletier-Simpson (D) **Introduced:** 05/12/05 **Enacted:** 06/10/05 **Act/Chapter Number:** 379 **Breach Provisions Effective:** 01/31/06 **Enforcement:** Appropriate state regulator action for licensed/regulated info. brokers; AG action for all other info. brokers. **Penalties:** Up to $500 fine per violation up to $2.5K for each day information broker is in violation; equitable relief; enjoinment. **Summary:** Requires info. broker engaged in business in Maine that is in possession of electronic data containing personal info. to disclose any unauthorized acquisition or suspected unauthorized acquisition of that personal info. to a person whose personal info. may have been acquired. Report due 02/01/06 addressing business data security and security breaches. **State agency** security breaches not specifically addressed in act, governmental agencies whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes are exempt from "info. broker" definition. Report due 02/01/06 addressing security of information maintained by State Government. http://janus.state.me.us/legis/ros/lom/LOM123rd/9Pub351-400/Pub351-378.htm#P1036_197584	**Info. broker** that maintains computerized data including personal info. Info. broker defined as person who for monetary fees/dues engages in business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring or communicating individual's info. for primary purpose of furnishing to nonaffiliated 3rd parties. **Security breach** defined as unauthorized acquisition of individual's computerized data that compromises security, confidentiality or integrity of individual's personal info. maintained by info. broker. Good faith acquisition of personal info. by info. broker employee or agent for purposes of info. broker is not system security breach if personal info. is not used for or subject to unauthorized disclosure.	**Trigger** Personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $5K; or • affects more than 1000 people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted or redacted: • SS # • State DL# or ID# • account, credit card or debit card # if usable w/out additional identifying info., access codes or passwords • account passwords or personal ID #s or other access codes • any above items when not in connection with individual's first name or first initial and last name, if info. compromised would be sufficient to perform or attempt to perform ID theft. Excludes info. publicly available from government records or widely distributed media.	Delay for law enforcement **Investigation.** **No safe harbor** provision.	**3rd Party Notice** Person that maintains computerized data not owned on behalf of info. broker, and data includes personal info., shall notify info. broker of any data security breach following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. When security breach notification is required, info. broker must also notify appropriate state regulators within Dept. of Professional and Financial Regulation, or AG if info. broker not [illegible] by Dept. [illegible] required for more than 1,000 persons at a time, then info. broker also must notify CRAs	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Minnesota H 2121 **Sponsor:** Johnson J (R) **Introduced:** 3/29/05 **Enacted:** 06/02/05 **Act/Chapter Number:** 167 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action; private right of action. **Penalties:** Investigation; injunction; civil penalties up to $25K; actual damages; investigation costs; reasonable attorney's fees; other equitable relief. **Summary:** Requires businesses to notify persons whose personal info. has been disclosed to unauthorized persons. **State agency** security breaches are addressed in enacted **2005 HF 225** (Chapter 163). http://www.revisor.leg.state.mn.us/bin/getpub.php?pubtype=STAT_CHAP&year=2005&chapter=167	Person/business that conducts business in MN and owns or licenses any data that includes personal info. Security breach defined as unauthorized acquisition of computerized data compromising security, confidentiality, or integrity of personal info. maintained by person/business. Good faith acquisition of personal info. by person/business employee or agent for purposes of person/business is not security system breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements is not encrypted • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info publicly available from federal, state or local government records	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person/business that maintains computerized data including personal info. not owned shall notify information owner/licensee of any security breach of data following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 500 persons at a time, then also must notify CRAs **within 48 hours** of notice timing, distribution and content.	**Exempts from chapter** financial institutions as defined by US Code Title 15, section 6809(3), GLBA Title V.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Montana H 732 **Sponsor:** Roberts (R) **Introduced:** 02/15/05 **Enacted:** 04/28/05 **Act/Chapter Number:** 518 **Breach Provisions Effective:** 03/01/06 **Enforcement:** AG action. **Penalties:** investigation; injunction; restrainment; voluntary compliance; civil fines up to $10K. **Summary:** Requires businesses to report a breach of computer security. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions related to credit report blocks, credit card solicitation/renewal protections, and destruction of business records. http://data.opi.state.mt.us/bills/2005/billhtml/HB0732.htm	Person or business that conducts business in MT and owns or licenses computerized data that includes personal info. **Security breach** defined as unauthorized acquisition of computerized data that materially compromises security, confidentiality or integrity of personal info. maintained and causes or is reasonably believed to cause loss or injury to a Montana resident. Good faith acquisition of personal info. by employee/agent of person/business for purposes of person/business is not data system security breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written, electronic or telephonic. **Timing** Without unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**, but law enforcement agency must specifically request notification delay. **Safe harbor** for providing notice pursuant to internal info. security policy that does not unreasonably delay notice.	**3rd Party Notice** Person/business that maintains computerized data including personal info. not owned shall notify information owner/licensee of any security breach of data immediately following discovery if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice to Montana resident implies individual may obtain report from CRA, then business shall coordinate with CRA on timing, content and distribution of notice.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Nevada A 1a **Sponsor:** Assembly Committee of the Whole **Introduced:** 6/07/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 6 **Breach Provisions Effective:** 06/17/05 **Enforcement:** N/A -see SB 347 **Penalties:** N/A -see SB 347 **Summary:** Makes technical corrections to certain legislative measures relating to protection of Social Security numbers, drivers licenses, ID cards and financial account numbers; amends measures relating to discipline of medical licensees, payday loans, collection agencies, felony DUI sentencing and credit unions. **Repeals enacted 2005 AB 334 (Chapter 486), Section 6, regarding business security breaches, and amends enacted 2005 SB 347, Section 21, regarding "personal info." definition.** http://www.leg.state.nv.us/22ndSpecial/bills/AB/AB1_EN.pdf	N/A -see SB 347	N/A -see SB 347	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password (employer identification # included in Section 21 of SB 347 as originally enacted is removed) Excludes info. that is publicly available.	N/A -see SB 347	N/A -see SB 347	N/A -see SB 347

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Nevada S 347 **Sponsor:** Wiener (D) **Introduced:** 3/25/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 485 **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG or county DA action. **Penalties:** Injunction; data collector may bring action against security breach perpetrator for damages/restitution. **Summary:** Requires data collectors provide notification of any breach of security involving system data. **State agency** security breaches are addressed in enacted **2005 AB 334** (Chapter 486). **Identity theft measure** also includes provisions related to financial forgery laboratories, credit card issuer identity theft policies, protection and destruction of business records containing personal info., electronic data encryption, and identity theft penalties. http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf	Data collector that owns or licenses computerized data which includes personal info. Data collector by definition includes financial institution. Security breach defined as unauthorized acquisition of computerized data that materially compromises security, confidentiality or integrity of personal info. maintained by data collector. Does not include good faith acquisition of personal info. by employee/agent of data collector for data collector's legitimate purpose, so long as personal info. is not used for purpose unrelated to data collector or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted: • SS or employer identification # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password (employer identification # removed via amendments in **AB 1A**) Excludes info. that is publicly available.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Data collector maintaining computerized data including personal info. data collector doesn't own must immediately notify information owner/licensee when breach is discovered if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 1,000 persons at a time, then also must notify CRAs of time notification is distributed and notification content.	**In compliance with chapter's security breach notification section** for persons subject to and in compliance with GLBA.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New Jersey A 4001 **Sponsor:** Watson-Coleman (D) **Introduced:** 05/05/05 **Enacted:** 09/22/05 **Act/Chapter Number:** 2005-226. **Breach Provisions Effective:** 01/01/06 **Enforcement:** AG action, private right of action. **Penalties:** Injunction; civil penalties up to $10K for 1st offense and up to $20K for 2nd and each subsequent offense; damages; reasonable attorneys' fees, filing fees and reasonable costs of suit. **Summary:** Requires notification of unencrypted personal info. da'a security breaches. **State agency** security breaches included in act via "public entity" definition. **Identity theft measure** includes provisions related to identity theft related police reports and judicial determinations of factual innocence, identity theft victim database, security freezes, CRA's release of consumer's credit header info., business disposal of consumer's personal info., and SSN use restrictions. http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM	Business or public entity doing business in NJ that compiles or maintains computerized records that include personal info. **Security breach** defined as unauthorized access to electronic files, media or data containing personal info. that compromises security, confidentiality or integrity of personal info. when access to personal info. has not been secured by encryption or by any other method or technology that renders personal info. unreadable or unusable. Good faith acquisition of personal info. by employee/ agent of business for legitimate business purpose is not breach of security, provided personal info. is not used for purpose unrelated to business or subject to further unauthorized disclosure.	**Trigger** Personal info. was or is reasonably believed to have been accessed by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements. • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password • dissociated data, if linked, and means to link dissociated data is accessed in connection with access to dissociated data Excludes personal info. made available to general public from federal, state or local government records, or widely distributed media.	Delay for law enforcement **investigation**, but law enforcement agency must specifically request notification delay. Notice not required if business or public entity establishes that misuse of info. is not reasonably possible. Determination must be documented in writing and maintained for 5 years. Safe harbor for providing notice pursuant to an internal info security policy and notification is consistent with state requirements.	**3rd Party Notice** Business or public entity compiling or maintaining computerized records including personal info. on behalf of another business or public entity must immediately notify business or public entity, who shall notify its NJ customers when breach is discovered, if personal info. was or is reasonably believed to have been accessed by unauthorized person. If notice required, must report to Division of State Police in Department of Law and Public Safety prior to notifying customers. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notices' timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York City 0141-2004 **Sponsor:** NYC Council Member **Introduced:** 02/04/04 **Enacted:** 05/19/05 **Act/Chapter Number:** **Breach Provisions Effective:** 09/20/05 **Enforcement:** NYC Commissioner civil action. **Penalties:** Fine of not more than $500; civil penalty of $100 for each violation. **Summary:** Requires businesses to notify consumers in the event of a security breach of personal identifying info. **Identity theft measure** also includes provisions related to disposal of records containting consumer's personal info. http://webdocs.nyccouncil.info/textfiles/Int%200141-2004.htm	Any person required to be licensed by Department of Consumer Affairs, or pursuant to provisions of state law enforced by Department, that owns/leases, or maintains but does not own, data that includes personal identifying info. Security breach defined as unauthorized possession of personal identifying info. that compromises security, confidentiality or integrity of such info. Good faith or inadvertent possession of any personal identifying info. by employee/agent of licensee for legitimate purposes of business of licensee shall not constitute breach of security.	Trigger Personal identifying info. was or is reasonably believed to have been acquired by an unauthorized person. Method Written, electronic or telephonic. Timing As soon as practicable by method reasonable under the circumstances. Substitute Trigger Disclosure is impracticable or inappropriate given circumstances of breach and victims' identity. Substitute Method Via mechanism of licensee's choosing provided mechanism is reasonably targeted to individual in manner that does not further compromise integrity of personal info. disclosed and has been approved, or is in compliance with rules promulgated, by Commissioner.	Includes all of the following data, notwithstanding method by which such information is maintained: • DOB • SS # • State DL or ID # • financial account, credit card, debit card, ATM # or code • personal ID # • mother's maiden name • comptr passwrd • elec. signature • biometric data	No safe harbor provision.	3rd Party Notice Person required to be licensed by Consumer Affairs Dept., or pursuant to provisions of state law enforced by Dept. that maintains but does not own data that includes personal identifying info. must notify data owner, lessor or licensor when security breach is discovered, if personal identifying info. was or is reasonably believed to have been acquired by unauthorized person. Must immediately disclose to Department of Consumer Affairs and police department any security breach following discovery of such breach if such personal identifying info. is reasonably believed to have been acquired by unauthorized person.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York A 4254A **Sponsor:** Brennan (D) **Introduced:** 02/09/05 **Enacted:** 08/09/05 **Act/Chapter Number:** 442 **Breach Provisions Effective:** 12/07/05 **Enforcement:** AG action. **Penalties:** Injunction; enjoinment; restrainment; actual damages, including consequential financial losses, if notification was not provided, if court determines violation occurred knowingly/recklessly, allowed civil penalties of greater of $5K or $10 per instance of failed notification up to $150K. **Summary:** Requires any state agency or business which owns or licenses a computerized database which includes vulnerable personal info. shall disclose any breach of security of such system to any resident of New York state whose unencrypted personal info. may have been acquired by an unauthorized person. **Preempts** local laws, ordinances and codes. **State agency** security breaches addressed in Section 3 of act. See enacted **2005 S 5827** (Chapter 491) for additional clarification. http://assembly.state.ny.us/leg/?bn=A04254&sh=t	Person or business that conducts business in NY and owns or licenses computerized data that includes personal info. Security breach defined as unauthorized acquisition or acquisition without valid authorization of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by business. Good faith acquisition of personal info. by employee or agent of business for purposes of business is not a security breach, provided private info. is not used or subject to unauthorized disclosure.	Trigger Unencrypted private info. is reasonably believed to have been acquired by unauthorized person. See enacted **2005 S 5827** (Chapter 491) for clarification. Method Written, telephonic, or electronic for person who has expressly consented to electronic notice. Log required for electronic/telephonic notice. ***Statute specifies notice content.*** Timing Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. Substitute Trigger • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. Substitute Method Email, website posting and major statewide media notification.	Private info. in combination with any one or more of following data elements, when either personal info. or data element is not encrypted or encrypted with an encryption key that has also been acquired: • SS # • State DL# or ID# • non-driver ID # • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records. "Personal info." shall mean any info. concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.	Delay for law enforcement **investigation**. No safe harbor **provision**.	3rd Party Notice Person or business maintaining computerized data including private info. not owned must immediately notify owner or licensee upon breach discovery if private info. was or is reasonably believed to have been acquired by unauthorized person. If any notice required, AG, Consumer Protection Board and Cyber Security and Critical Infrastructure Coord. Office must be notified of timing, distribution and content of notice and approximate number affected. If notice required for more than 5,000 persons at a time, then also must notify CRAs of notice timing, distribution, content and approximate number of affected persons. **CRA notification not limited to 3 major CRAs - AG will compile CRA list.**	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
New York S 5827 **Sponsor:** Fuschillo (R) **Introduced:** 06/19/05 **Enacted:** 08/09/05 **Act/Chapter Number:** 491 **Breach Provisions Effective:** 12/07/05 **Enforcement:** AG action. **Penalties:** N/A - see **A 4254**. **Summary:** Makes technical changes to certain provisions of Info. Security Breach and Notification Act; clarifies definition of breach of security system; changes reference of person or entity to state entity in Section 3; provides for telephone notification to affected persons and log of each notification; clarifies awarding of damages. http://assembly.state.ny.us/leg/?bn=S05827&sh=t	N/A - see **A 4254**.	Trigger Such business may consider following factors, among others: (1) indications that info. is in physical possession and control of un-authorized person, such as lost or stolen computer or other device containing info.; or (2) indications that info. has been downloaded or copied; or (3) indications that info. was used by unauthorized person, such as fraudulent accounts opened or instances of ID theft reported.	N/A - see **A 4254**.	N/A - see **A 4254**.	N/A - see **A 4254**.	N/A - see **A 4254**.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
North Carolina S 1048 **Sponsor:** Clodfelter (D) **Introduced:** 03/24/05 **Enacted:** 09/21/05 **Act/Chapter Number:** 2005-414. **Breach Provisions Effective:** 12/01/05 **Enforcement:** AG action; private right of action limited to injured individuals. **Penalties:** Injunction; $5K civil penalty per violation, attorney fees; treble damages for injured consumer. **Summary:** Requires notification of personal info. security breaches. **State agency** security breaches not addressed in act. "Business" definition specifically exempts state agencies. **Identity theft measure** also includes provisions related to security freezes, business disposal of consumer's personal info., and SSN use restrictions. http://www.ncleg.net/Sessions/2005/Bills/Senate/HTML/S1048v6.html	Business that owns or licenses personal info. of NC residents or business that conducts business in NC that owns/licenses personal info. in any form, **whether computerized, paper, otherwise.** Security breach is defined as unauthorized access to and acquisition of unencrypted & unredacted records or data (or encrypted records/ data along with confidential process/key) containing personal info. where illegal use has occurred or is reasonably likely to occur or that creates material risk of harm to consumer. Good faith acquisition of personal info. by employee/agent of business for legitimate purpose is not security breach, provided that personal info. is not used for purpose other than lawful business and is not subject to further unauthorized disclosure.	**Trigger** Personal info. was acquired by unauthorized person where illegal use of personal info. has occurred or is reasonably likely to occur or that creates material risk of harm to consumer. **Method** Written, telephonic or electronic for person who has expressly consented to electronic notice. ***Statute specifies notice content.*** **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written, electronic or telephonic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with identifying info. as defined in G.S. 14-113.20(b): • SS # • State DL# • Checking, savings, credit/debit card #s • PIN code • biometric data • fingerprints • digital signature • passwords • electronic ID #s, email names or addresses, Internet account numbers or identification names, parent's legal surname prior to marriage, or password if it would permit access to person's financial account or resources. Excludes personal info. available to general public from federal, state or local government records; and publicly available directories containing info. individual has voluntarily consented to have publicly disseminated.	Delay for law enforcement **investigation**, provided law enforcement agency delay request is made in writing or business documents such request contemporaneously in writing, including name of law enforcement officer making request and officer's law enforcement agency engaged in investigation. No **safe harbor** provision.	**3rd Party Notice** Business that maintains or processes records/data including personal info. on behalf of personal info. owner or licensee must immediately notify owner or licensee upon breach discovery consistent with law enforcement needs. If notice required for more than 1,000 persons at a time, then also must notify AG's office and CRAs of notice timing, distribution and content.	**In compliance with act's security breach section** for financial institutions subject to and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
North Dakota S 2251 **Sponsor:** Trenbeath (R) **Introduced:** 01/17/05 **Enacted:** 04/22/05 **Act/Chapter Number:** 447 **Breach Provisions Effective:** 06/01/05 **Enforcement:** AG action; private right of action. **Penalties:** Investigation; injunction; restrainment; civil penalties of $1-5K per violation; damages and adjudicative proceeding/hearing costs; treble damages. **Summary:** Requires disclosure to consumers of a breach in security by businesses maintaining personal identifying info. in electronic form. **State agency** security breaches not addressed in act. http://www.legis.nd.gov/assembly/59-2005/session-laws/documents/SALES.pdf#CHAPTER447	Any person that conducts business in ND and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of computerized data when access to personal info. has not been secured by encryption or any other method or technology that renders electronic files, media, or data bases unreadable/ unusable. Good-faith acquisition of personal info. by employee/agent of person is not a system security breach if personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when name and data elements are not encrypted • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password • DOB • mother's maiden name • employee ID # • electronic signature Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice Person that maintains computerized data including personal info. on behalf of personal info. owner or licensee must immediately notify owner or licensee upon breach discovery, if personal info. was or is reasonably believed to have been acquired by an unauthorized person.	**In compliance with chapter** for financial institutions subject to, examined for, and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Ohio H 104 **Sponsor:** Martin (R) **Introduced:** 03/01/05 **Enacted:** 11/17/05 **Act/Chapter Number:** 43 **Breach Provisions Effective:** 02/17/06 **Enforcement:** AG action. **Penalties:** Investigation, restrainment, injunction; costs; civil penalties for intentional/reckless noncompliance of $1K/day up to 60 days of noncompliance, $5K/day after 60 days, and $10K/day after 90 days. **Summary:** Requires disclosure to consumers of a breach in security by businesses maintaining personal identifying info. in electronic form. **Preempts** all rules, regulations, resolutions, codes, and ordinances of all counties, municipal corporations, townships, and agencies of counties, municipal corporations, and townships. **State agency** security breaches addressed in Section 1, Subsection 1347.12, of act. http://www.legislature.state.oh.us/bills.cfm?ID=126_HB_104	Person that conducts business in OH and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized access to and acquisition of computerized data that compromises security or confidentiality of personal info. owned/licensed by person and that causes, reasonably is believed to have caused, or reasonably is believed will cause material risk of ID theft or other fraud to person or property of resident of state. Good-faith acquisition of personal info. by employee/agent of person is not a system security breach if personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted, unredacted, or altered to be unreadable personal info. was or is reasonably believed to have been accessed/acquired by unauthorized person, if such causes or reasonably is believed will cause material risk of ID theft or other fraud to resident. **Method** Written, electronic (if primary method of communication), telephonic, or via contract provision that doesn't conflict with any section provision. **Timing** **No later than 45 days from breach discovery or notification** and within most expedient time possible consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and ***specified*** major statewide media notification.	Individual's first name or first initial and last name in combination with and linked to any one or more of following data elements, when data elements are not encrypted, redacted, or altered by any method or technology in such manner that data elements are unreadable: • SS # • State DL# or ID# • account, credit card or debit card # in combination with and linked to required access/security code or password Excludes info. publicly available from federal, state or local government records, or specified media that are widely distributed.	Delay for law enforcement **investigation**. **No safe harbor provision.**	**3rd Party Notice** Person that is custodian or stores computerized data including personal info. shall notify owner or governmental entity of any system security breach in expeditious manner, if personal info. was or reasonably is believed to have been, accessed and acquired by unauthorized person and if such causes or reasonably is believed will cause material risk of ID theft or other fraud to resident. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	**Exempts from act's security breach notification section** any financial institution, trust company, or credit union or any affiliate of financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Pennsylvania S 712 **Sponsor:** Wonderling (R) **Introduced:** 06/03/05 **Enacted:** 12/22/05 **Act/Chapter Number:** 2005-94 **Breach Provisions Effective:** 06/20/06 **Enforcement:** AG action; private right of action. **Penalties:** Civil penalties of $1-5K per violation; actual damages, treble damages; reasonable costs and attorney fees. **Summary:** Provides for the notification of residents whose personal information data was or may have been disclosed due to a security system breach. Relates to data that materially compromises the security or confidentiality of personal information. Imposes penalties. Allows telephonic notice under certain circumstances. Requires notice of the breach if encrypted information is accessed in an unencrypted form. Relates to vendor notification regarding breach of a security system. **Preempts** all rules, regulations, codes, statutes or ordinances of all cities, counties, municipalities and other local agencies within Commonwealth regarding matters expressly set forth in Act. **State agency** security breaches included in act via "entity" definition. http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf	Entity that conducts business in PA and maintains, stores or manages computerized data that includes personal info. Security breach is defined as unauthorized access and acquisition of computerized data that materially compromises security or confidentiality of personal info. maintained by entity as part of database of personal info. regarding multiple individuals and that causes or entity reasonably believes has caused or will cause loss/injury to any state resident. Good faith acquisition of personal info. by entity employee or agent for purposes of entity is not system security breach if personal info. is not used for purpose other than lawful purpose of entity and is not subject to further unauthorized disclosure.	**Trigger** Unencrypted or unredacted personal info. was or is reasonably believed to have been accessed/acquired by unauthorized person. **Method** Written, telephonic (if customer can reasonably expect to receive and specified info. is provided), or email (prior business relationship only). **Timing** Notice shall be made without unreasonable delay, except for law enforcement investigation delay or in order to take any measures necessary to determine scope of breach and to restore data system's reasonable integrity. **Substitute Trigger** • cost exceeds $100K; or • affects more than 175K people, or • no sufficient contact info. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following unencrypted or unredacted data elements: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement agency **investigation** if agency determines and advises enity in writing. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with Act's notification requirements.	**3rd Party Notice** Vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any system security breach following discovery by vendor to entity on whose behalf vendor maintains, stores or manages data. Entity shall be responsible for making determinations and discharging any remaining duties under Act. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and number.	**In compliance with act** for financial institutions subject to and in compliance with federal interagency banking notification guidance, or entity in compliance with notification requirements pursuant to rules, regulations, procedures or guidelines established by entity's primary or functional Federal regulator.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Rhode Island H 6191A **Sponsor:** Gemma (D) **Introduced:** 03/09/05 **Enacted:** 07/10/05 **Act/Chapter Number:** 225 **Breach Provisions Effective:** 03/01/06 **Enforcement:** AG action. **Penalties:** Civil fines of not more than $100 per occurrence up to $25K. **Summary:** Requires disclosure of computerized unencrypted personal info. data security breaches. **State agency** security breaches included in act. http://www.rilin.state.ri.us/PublicLaws/law05/law05225.htm	Any state agency or person doing business in RI that owns, maintains or licenses computerized data that includes personal info. **Security breach** is defined as unauthorized acquisition of unencrypted computerized data compromises the security,confidentiality, or integrity of personal info. maintained by state agency or person. Good faith acquisition of personal info. by employee/agent of agency/person for purposes of agency/person is not system security breach, provided personal Info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person or person without authority to acquire said info., and such breach poses significant risk of ID theft. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent w/ law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $25K, or • affects more than 50K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Does ***not*** exclude info. that is publicly available.	Delay for law enforcement **investigation**. Notification not required if after appropriate **investigation** or after consultation with relevant federal, state, or local law enforcement agencies, determination is made that breach has not and will not likely result in significant risk of ID theft to individuals whose personal info. has been acquired. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	3rd Party Notice State agency or person that maintains computerized unencripted data including personal info. that state agency or person does not own shall notify owner or licensee of info. of any data security breach which poses significant risk of ID theft immediately following discovery, if personal info. was or is reasonably believed to have been acquired by unauthorized person.	**In compliance with chapter's security breach notification requirements** for any person that maintains security breach procedure pursuant to rules, regulations, procedures or guidelines established by primary or functional regulator, as defined in 15 USC 6809(2) and provides notice in accordance thereto when breach occurs. **In compliance with chapter** for financial institutions or their affiliates subject to, examined for, and in compliance with federal interagency banking guidance.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Tennessee S 2220 **Sponsor:** Herron (D) **Introduced:** 02/17/05 **Enacted:** 06/18/05 **Act/Chapter Number:** 473 **Breach Provisions Effective:** 07/01/05 **Enforcement:** AG action, private right of action. **Penalties:** Injunction; restrainment; enjoinment; civil penalties of whichever of following is greater: $10K, $5K/day for each day person's ID has been assumed, 10 times amount obtained or attempted to be obtained by person using ID theft, civil penalties up to $5K per knowing and willful violation; attorneys' fees and costs; damages, including treble. **Summary:** Requires persons, businesses or government agencies that discover a breach of info. security resulting in disclosure of unencrypted personal info. about persons to unauthorized third parties to provide notice of such disclosure. **State agency** security breaches included in act via "info. holder" definition. http://www.legislature.state.tn.us/bills/currentga/Chapter/PC0473.pdf	"Info. holder" (person or business) that conducts business in TN and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of unencrypted computerized data that materially compromises security, confidentiality, or integrity of personal info. maintained by info. holder. Good faith acquisition of personal info. by employee/ agent of info. holder for purposes of info. holder is not system security breach, provided personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/o unreasonable delay consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people; or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL # • • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Info. holder that maintains computerized data including personal info. not owned shall notify owner or licensee of info. of any data security breach if personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 1,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	**Exempts from chapter** financial institutions subject to GLBA Title V.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Texas S 122 **Sponsor:** Hinojosa (D) **Introduced:** 01/11/05 **Enacted:** 06/17/05 **Act/Chapter Number:** 294 **Breach Provisions Effective:** 09/01/05 **Enforcement:** AG action. **Penalties:** Restrainment; injunction; civil penalties of $2-50K per violation; reasonable expenses, attorney's fees, court and investigatory costs. **Summary:** Requires notification of unencrypted computerized personal info. data security breaches. **State agency** security breaches not addressed in act. **Identity theft measure** also includes provisions requiring businesses protect/safeguard any personal identifying info. collected/maintained, and to implement/maintain reasonable procedures, including taking any appropriate corrective action to prevent unlawful use of any personal identifying info. (exempts financial institutions as defined by 15 U.S.C. Section 6809(3). http://www.capitol.state.tx.us/cgi-bin/tlo/textframe.cmd?LEG=79&SESS=R&CHAMBER=S&BILLTYPE=B&BILLSUFFIX=00122&VERSION=5&TYPE=B	Person that conducts business in TX and owns or licenses computerized data that includes sensitive personal info. Security breach is defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of sensitive personal info. maintained by person. Good faith acquisition of sensitive personal info. by employee agent of person or business for purposes of person is not system security breach unless sensitive personal info. is used or disclosed by person in unauthorized manner.	**Trigger** Sensitive personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** As quickly as possible consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K; or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following items, if name and items are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation**. **Safe harbor** for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person that maintains computerized data including sensitive personal info. not owned shall notify owner or licensee of info. of any data security breach if sensitive personal info. was or is reasonably believed to have been acquired by unauthorized person. If notice required for more than 10,000 persons at a time, then also must notify CRAs of notice timing, distribution and content.	None.

GENERAL INFO.	COMPLIANCE	NOTICES	COVERED INFO	NOTICE EXCEPTIONS	ADDITIONAL NOTICE REQUIRED	OTHER LAW EXCEPTIONS
Washington S 6043 **Sponsor:** Brandland (R) **Introduced:** 2/24/05 **Enacted:** 05/10/05 **Act/Chapter Number:** 368 **Breach Provisions Effective:** 07/24/05 **Enforcement:** Private right of action. **Penalties:** Damages; enjoinment. **Summary:** Requires disclosure of any breach of security of a system following discovery by any agency or business who computerizes data that includes personal info. to the resident of this state whose unencrypted personal info. was, or is reasonably believed to have been, acquired by an authorized person. **State agency** security breaches addressed in Section 1 of act http://www.leg.wa.gov/pub/billinfo/2005-06/Pdf/Bills/Session%20Law%202005/6043-S.sl.pdf	Person or business that conducts business in WA and owns or licenses computerized data that includes personal info. Security breach is defined as unauthorized acquisition of computerized data that compromises security, confidentiality, or integrity of personal info. maintained by person/ business. Good faith acquisition of personal info. by employee/agent of person/business for purposes of person/business is not system security breach when personal info. is not used or subject to further unauthorized disclosure.	**Trigger** Unencrypted personal info. was or is reasonably believed to have been acquired by an unauthorized person. **Method** Written or electronic. **Timing** Most expedient time possible w/out unreasonable delay,consistent with law enforcement needs or other necessary measures. **Substitute Trigger** • cost exceeds $250K, or • affects more than 500K people, or • not enough info to provide written/ electronic notice. **Substitute Method** Email, website posting and major statewide media notification.	Individual's first name or first initial and last name in combination with any one or more of following data elements when either name or data elements are not encrypted: • SS # • State DL# or ID# • account, credit card or debit card # in combination with required access/security code or password Excludes info. publicly available from federal, state or local government records.	Delay for law enforcement **investigation.** Notice not required for technical breach not reasonably likely to subject customers to risk of criminal activity. Safe harbor for providing notice pursuant to an internal info. security policy and notification is consistent with state timing requirements.	**3rd Party Notice** Person or business that maintains computerized data including personal info. not owned shall notify owner or licensee of info. of any data security breach if personal info. was or is reasonably believed to have been acquired by unauthorized person.	None.

Comparison of State Security Breach Notification Laws

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Arkansas	Commercial, charitable, educational, or nonprofit entities including state agencies	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached if entity suffering breach determines breach presents a reasonable likelihood of harm to customers.	None	State AG	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	No
California	Any person, government agency or business that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Connecticut	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Delaware	Persons who conduct business in the state that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code, medical information	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Must promptly provide written notification of the nature and circumstances of breach to Consumer Protection Division of the Department of Justice	State AG, Consumer Protection Division of the Department of Justice	Does not apply to entity regulated by state or federal law that provides greater protection to personal information	Yes, treble damages plus attorney fees
Florida	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification within 45 days following discovery of breach to individuals whose unencrypted computerized data containing personal information breached. Notification not required if after consultation with federal/state/local agencies responsible for law enforcement, business determines harm to consumers not likely as a result of breach	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Legal Affairs. Penalties for non-notification increase with time since security breach	None	No
Georgia	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 10,000 individuals	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Illinois	Data collection including government agencies, educational institutes, public and private entities that collects, handles, or disseminates nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	Yes
Indiana	State agencies holding computerized personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG	None	No
Louisiana	Persons who conduct business in the state including state agencies, that owns or licenses computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	None	State AG	None	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Maine	Information brokers	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must notify appropriate state regulator of breach, must also coordinate with CRAs if breach includes information on at least 1,000 individuals	Department of Professional and Financial Regulation, State AG for information brokers not regulated by Department of Professional and Financial Regulation	None	No
Minnesota	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs if breach includes information on at least 500 individuals	State AG	Does not apply to financial institutions or HIPAA entities	No
Montana	Persons who conduct business in the state and maintains computerized data containing personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Agency suffering breach must coordinate with CRAs	Consumer Protection Office	Insurance-support organizations follow same breach laws, but Montana Insurance Commissioner has authority	No

State	Entities Covered	Information Covered	Notification Requirements	Further Duties	Enforcement	Exemptions	Private Right of Action
Nevada	Data collectors: includes business entities, government agencies, educational institutions, and associations who handle, collect, or disseminate nonpublic personal information	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals	State AG or a district attorney of any county	Data collectors in compliance with GLB exempted	No
New Jersey	Commercial, charitable, or nonprofit entities including state, county, or local government entities	Personal information: Name + SSN, DL, account number/identifier with access code	Notification without unreasonable delay to individuals whose unencrypted computerized data containing personal information breached unless entity suffering breach establishes that misuse of information is not reasonably possible. Must keep written documentation of evidence for 5 years	Entity suffering breach must coordinate with CRAs if breach includes information on at least 1,000 individuals. Must also notify State Police in advance of disclosure of breach	State AG	None	No