

# MICROFILM DIVIDER

OMB/RECORDS MANAGEMENT DIVISION

SFN 2053 (2/85) 5M



ROLL NUMBER

DESCRIPTION

2251

2005 SENATE JUDICIARY

SB 2251

2005 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2251

Senate Judiciary Committee

☐ Conference Committee

Hearing Date February 1, 2005

Tape Number	Side A	Side B	Meter #
1	X		2651 - End
1		X	670 - 840
Committee Clerk Signature <i>Maria L. Salby</i>			

Minutes: Relating to use of personal identifying info involving conduct outside of ND.

**Senator John (Jack) T. Traynor**, Chairman called the Judiciary committee to order. All

Senators were present. The hearing opened with the following testimony:

**Testimony In Support of the Bill:**

**Wayne Stenehjem** - ND Attorney General - Introduced the bill. (meter 2630) Chief among the problems this bill is designed to address is the growing difficulties of Identity theft. ID Theft is the fastest growing white collar crime in the US. Evidence indicates the 500,000 American this year alone will be will be victims of ID theft. It takes about 600 hours for the average victim to undo the damage that is done. The average perpetrator nets approximately \$40-92 thousand dollars. We need to have legislation in ND to meet the challenge of the originality of the thief. Due to the Internet no one is safe. An operation called dumpster diving-were they literally go into your dumpster for your information. Another new process on the scene is called "phishing".

See Att. #2. It appears to be a "security" type of issue on your computer asking you to confirm

Page 2

Senate Judiciary Committee

Bill/Resolution Number SB 2251

Hearing Date February 1, 2005

you personal information. (meter 2890). 5-10% of emails fall for this trick. The following two bills are to protect you from these scams. Last session we eliminated credit card numbers being on the cash register receipts. We also removed social security numbers off of all documents ie. drivers licenses

Do Not Call loop- hole. We have had 249 calls of violation. We have had 53 do not call investigations. 60% of ND is on the do not call list. ND has one of the best, broadest do not call list in the nation. Federal trade commission used to enforce it for 90 days. The FCC has changed it to 30 days. We would like to track the same time frame of 30 days.

We have fines of \$28,000 against violators.

I.D. theft is more of a violation then steeling a car or a bike. People who have had their ID stolen strongly feel that their privacy has been violated. It is a serious and personal crime. This bill also consolidated venues of counties. The judge can be aware of how far the perpetrators crime is.

**Sen. Trenbeath** questioned section 5, is chapter 51-15 some sort of civil remedy? Yes that is the Attorney Generals enforcement for consumer protection violations.

**Perrell D. Grossman** - Attorney Generals Consumer Protection Division. (meter 3858) Gave testimony - Att. #3. While we have received many calls on this problem we have no penalty for this and this bill will do that.

**Rep Aarsvold**, Dist #20, Gave Support on the bill.

**Darin Meschke**, Dir of Division of vital records (meter 5600) Gave testimony - Att. #3.

Submitted and Amendment - Att. #4.

Brochure - Att. #5

Page 3

Senate Judiciary Committee

Bill/Resolution Number SB 2251

Hearing Date February 1, 2005

**Testimony in Opposition of the Bill:**

none

**Senator John (Jack) T. Traynor**, Chairman closed the Hearing.

**Senator John (Jack) T. Traynor**, Chairman reopened the Hearing. (Tape 1, side 2, meter 670)

**Sen. Trenbeath** made the motion to do pass Amendment - Att #4, **Senator Triplett** seconded the motion. All were in favor, motion carries.

**Senator Hacker** made the motion to Do Pass As Amended and **Sen. Nelson** seconded the motion. All were in favor, motion carries.

Carrier: **Senator Syverson**

**Senator John (Jack) T. Traynor**, Chairman closed the Hearing

Date: 2/1/05  
Roll Call Vote #: 1

2005 SENATE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 225/

Senate Judiciary Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number \_\_\_\_\_

Action Taken Move to Amend AH #4

Motion Made By Sen. Trenbeath Seconded By Sen. Triplett

Senators	Yes	No	SenatorsSen. Nelson	Yes	No
Sen. Traynor	✓		Sen. Nelson	✓	
Senator Syverson	✓		Senator Triplett	✓	
Senator Hacker	✓				
Sen. Trenbeath	✓				

Total (Yes) 6 No 0

Absent 0

Floor Assignment \_\_\_\_\_

If the vote is on an amendment, briefly indicate intent:

Date: 2/1/05  
Roll Call Vote #: 2

2005 SENATE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 2251

Senate Judiciary Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number \_\_\_\_\_

Action Taken Do Pass As Amended

Motion Made By Sen. Hacker Seconded By Sen Nelson

Senators	Yes	No	SenatorsSen. Nelson	Yes	No
Sen. Traynor	✓		Sen. Nelson	✓	
Senator Syverson	✓		Senator Triplett	✓	
Senator Hacker	✓				
Sen. Trenbeath	✓				

Total (Yes) 6 No 0

Absent 0

Floor Assignment sen. Syverson

If the vote is on an amendment, briefly indicate intent:

**REPORT OF STANDING COMMITTEE**

**SB 2251: Judiciary Committee (Sen. Traynor, Chairman) recommends AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2251 was placed on the Sixth order on the calendar.

Page 1, after line 21, insert:

"j. An individual's birth, death, or marriage certificate."

Renumber accordingly



2005 HOUSE JUDICIARY

SB 2251

2005 HOUSE STANDING COMMITTEE MINUTES  
BILL/RESOLUTION NO. SB 2251

House Judiciary Committee

☐ Conference Committee

Hearing Date 3/7/05

Tape Number	Side A	Side B	Meter #
1	xx		34-end
1		xx	0-13.7
1		xx	33.7-36
Committee Clerk Signature <i>Dawn Penrose</i>			

Minutes: 14 members present.

**Chairman DeKrey:** We will open the hearing on SB 2251.

**Wayne Stenehjem, Attorney General:** Support, I'm here to talk about SB 2251, which is related to the most serious and quickly increasing white collar crime in the country, and that is the issue of identity theft (see written testimony). Some states attorneys, especially in other areas, are not certain where the locus of the crime is, where the actual crime was committed, or you have a victim who lives in one state, a credit card issued in another state, and then you have a transaction that might take place in yet another state. So under this statute, it would say that if we have a victim here in ND, the ND courts are the place where the case could be prosecuted, and I think that's an important protection for our citizens. We have released, in our office, an enormous amount of information regarding what people can do to protect themselves from becoming victims of identity theft, and steps that can be taken in the event that is what happened. But no matter how careful a person is, it is unfortunate that it is just about impossible to totally

eliminate the possibility of becoming a victim of identity theft. A lot of identity theft takes place over the Internet and information that is obtained by people who live out of state, a lot of it occurs right here in ND, especially through an activity known as dumpster diving, where individuals will go to your trash can and look through it and see if you have telephone bills, discarded bank statements, those credit card applications that we get in the mail, and they utilize those to establish an identity, open up credit card accounts, telephone accounts, bank accounts, etc. I think this is a bill that will get tough on the issues. I'm happy to answer questions. I want to mention that there is one additional issue that I hope this committee will be willing to consider, that dovetails onto this very question. You may have heard about the ChoicePoint scandal, that arose. ChoicePoint is a consumer information business that exists down in Georgia. They give information on individuals for job applications, insurance companies and credit purposes, etc. They had somebody posing as a legitimate businesses, who came in and obtained information from ChoicePoint and used that information. They used that information, we understand, to commit identity theft. The only reason that most people feel that anybody ever knew what happened at ChoicePoint, was that California has a statute that says when your security is breached in your business that collects this information, you have to notify the consumer. No other state, at that point, had a statute that says if there is a breach of that information, you have to tell the consumers, so that they can take action to get a copy of their credit report to see if their identity has been stolen, and so Parrell Grossman has some amendments that I hope this committee will be willing to consider to adopt that kind of legislation here in ND, like California has, like a number of states are looking at.

**Representative Delmore:** Why is it that credit card companies are so quick to simply pay the charges and do very little to investigate identity theft. My niece was a victim of it, she did her own fact finding and found out who it was and had done it. The company just decided that they would just absorb the cost. In the end result, it costs all of us as well. Have they gotten better about this.

**Wayne Stenehjem, Attorney General:** I think so, because I've been on panels where we discussed this problem, what the states are doing, what the credit card companies are doing. They are undergoing some massive efforts to get a handle and catch these people, because they don't want to absorb the cost. Remember that if somebody opens up a credit card account in your name, you have to deal with getting your credit report in order and all those things, but you don't have to pay the money. The credit card company will absorb that cost and they're the ones that are losing that \$4 billion dollars. It certainly is in their economic interest to do everything they can to bring these people to justice and not simply absorb the cost. I think they are doing a better job. It's massive, when you have this number of crimes that is happening. It is very hard to get a handle on.

**Representative Delmore:** Should we put an emergency cause on it, or is that not a big deal.

**Wayne Stenehjem, Attorney General:** What a great idea.

**Representative Koppelman:** On lines 13 and 14, page 2, item #4, you say basically that the problem must be discovered within or acted upon within 6 years of when it is discovered. Does that lengthen the statute of limitations.

**Wayne Stenehjem, Attorney General:** The current statute of limitations is 3 years, and the reason for increasing it, I think, is because sometimes it is hard to discover. Sometimes you

don't know you're a victim for months or even years after the crime has been committed. So this lengthens it, not shortens it.

**Representative Koppelman:** I think it is good that credit card companies ask you some security questions when you call them. Every once in a while, though, one of those questions comes out of left field, and I've learned to ask did I give you that information, and a lot of times they'll say no, we're just trying to update our file. Which means that they are trying to get more and more information on you. Is there a standard in the industry, or is that even an issue or concern when it comes to identity theft, how much information is really needed.

**Wayne Stenehjem, Attorney General:** Constantly, because you can go to the grocery store, and pay with bank card and they know what I bought. This is an issue that is growing. I think it's particularly hard for us here in ND, because we're trusting and when people ask us for information, we're happy to chit chat with them, and we trust them and we need to be a lot more careful about the information we voluntarily give to anybody. Even when you fill in a warranty card when you buy a new computer or printer, and all they need to know is what did you buy, where did you buy it, and then your name and address. But they'll ask you what's your household income, etc. You don't have to answer those questions. You should put on those cards the information they really need to know and not all the extra stuff.

**Representative Boehning:** I've been getting a lot of calls from collection agencies, that somebody had gotten my number and they're calling me and asking for Susan. I called and checked up on my cell phone number, and 22 people have previously had my name or were registered under my name. When I talked to the collection agencies, they won't give me any information on any of the names. I can't remember how many I've had to straighten out already,

but they keep calling and saying that they are trying to get a hold with such and such. I don't know them. Is there any recourse that I can take to get those people.

**Wayne Stenehjem, Attorney General:** The first thing I would suggest is that as of last Tuesday, you can get a copy of your own credit report and I would suggest that that might be a wise thing for you to do. You can do that for free by going to [freecreditreport.com](http://freecreditreport.com) and ordering it. You get one free one per year from each of the three different credit reporting agencies. You should do that, start with one and in four months get one from the next company, and four months do that for the third one. You should do that every year and you might want to take a look to see if somebody is got something that needs to be looked at. We see a lot of, what is known as phishing, you can get it on your computer or it looks like E-bay, but it could be your bank, they say they are updating their security file, they have a logo from the bank or from e-bay and it looks very legitimate. Click here it says and you click, and of course, they want your bank account number, they want your password, they want your mother's maiden name, and all of that. They are identity thieves, and you should never, ever respond to e-mails that you get that ask you for information that those companies already have. The companies already have the information, and that's one of the fastest growing areas of identity theft, because it works, it's very legitimate looking and 5% of the people who get them actually respond and give them all that information they are asking for. In my case, they were going to close my e-bay account, and that was serious business.

**Representative Meyer:** What are the problems with identity theft, and I wish this bill could address it, and I don't believe it does, after a credit card company is notified, and they're not willing to just eat this usually, after a credit card company is notified that this is an identity theft

problem, what they do is just turn around and sell it to a collection agency, and after having a parent who's been a victim, we're going on a little more than 10 years, and we've gone to the states attorney and he said there is nothing in state law in ND that prohibits them from doing this. I wish it could be somehow in state law that once a credit card company is notified that this is an identity theft, they can no longer sell or transfer that information.

**Wayne Stenehjem, Attorney General:** A couple of things, we do have a law that says if you make a report and claim that a charge on your credit card is not legitimate, they have to stop collecting it, they can't do anything further with it, and they have to investigate it, and notify you and make that determination. The second thing is that under federal law, and now under state law, you can file a police report with my office. We've done what is called "Affidavit of Identity Theft" and that puts a freeze on the account from further charges.

**Representative Meyer:** There's nothing that prohibits them from going to a collection agency and saying, if you can get any.. and it creates such a harassment and he said there is nothing to stop them, true they have to be notified that there..

**Wayne Stenehjem, Attorney General:** And they have to stop trying to collect it, until they investigate and resolve the claim.

**Representative Meyer:** But their comment was, we aren't..

**Wayne Stenehjem, Attorney General:** My comment is that they have to. If there's an issue there, Representative Meyer, we'll be happy to try to look into it. I'm just outlining general rights that people have.

**Representative Meyer:** But they are prohibited from...

**Wayne Stenehjem, Attorney General:** They have to investigate it, and some people make complaints that a debt isn't due, and the debt is due. So they have to make an investigation of it and notify you what their determination is.

**Representative Meyer:** And at that time, they can no longer sell it to a collection agency.

**Wayne Stenehjem, Attorney General:** Then you have to exercise your other rights. If they ultimately decide that the bill is due, you have to pursue it in a regular way they do any debt; presumably up to and including going to court, where you present your defense to that.

**Representative Galvin:** As a career guidance counselor, you would say that identity theft is much more profitable than bank robbery.

**Wayne Stenehjem, Attorney General:** The statistics show that the average bank robber, who takes enormous risks to their health and safety, get very little; but identity thieves who are often, who knows where, can get \$50,000. We all need a dose of skepticism. We need to be more skeptical of people.

**Chairman DeKrey:** Thank you. Further testimony in support of SB 2251.

**Parrell Grossman, Director, Consumer Protection & Antitrust Division, Office of AG:** (see written testimony).

**Representative Koppelman:** In the ChoicePoint case, from what the AG said, even though they were located in GA, they were somehow required to comply with the requirement of the CA law. Would this allow us to do the same to reach beyond state lines, to require a company like this to disclose the information from the code.

**Parrell Grossman:** I think that's the first thing the AG mentioned, is when we talked about these amendments, was to make sure that we have the authority. We do have this authority.



ChoicePoint does business in ND, in fact, they access hundreds and hundreds of our ND drivers licenses, as evidenced by the fact that I am receiving many inquiries from ND drivers that are worried because an abstract has been issued on their drivers license. They do business in this state, they've chosen to do business and they are subject to all of our laws, including any law that this legislature enacts regarding notification pursuant to a security breach.

**Representative Boehning:** How do these companies get this information, they can just access this information, or do they need names and social security numbers, etc.

**Parrell Grossman:** In this case, as I indicated, it was really low tech. These individuals had bogus drivers license, created bogus identities, in one case I believe the individuals had fraudulent real estate licenses, and so they were purporting to be legitimate businesses that would have a legitimate need to access the information on file with ChoicePoint. In other words, a paying client for ChoicePoint, who now has the privilege for that payment, to access all of those records. So posing as legitimate business people themselves, they were able to buy a seat at the table with ChoicePoint and then have access to all the information that a legitimate company has access to, including these 19 billion public records. It appears that the circumstances were somewhat similar with Acxiom, two business associates of employees of Acxiom, gained very similar access to that company's records. It appears to not be difficult to obtain access to these kinds of databases, maintained by these companies. Now, I think ChoicePoint and others, are probably paying close attention and no doubt will enhance their security procedures. The question remains, that considering it has already happened on a fairly regular basis, will they be able to provide adequate protection to prevent this. If not, or even in occasional instances, in which they might fail to prevent those kinds of breaches, the Attorney General believes that

consumers must be notified. It remains a question in our mind, whether ChoicePoint would have notified ND consumers. There was some talk that ChoicePoint was only going to notify California consumers, and it was only after AG Stenehjem, and the other 18 attorneys general sent a letter demanding notification to the citizens in all of their affected states, that ChoicePoint said, oh yes, we were going to do that anyway. I leave that for your discretion, to decide whether ChoicePoint would have disclosed that information, whether they would have been concerned about the potential harm to about 137 potential victims in ND, when they were confronted with the release of confidential information involving over 35,000 Californians.

**Representative Boehning:** In other words, if I form a company and I pay a service fee to ChoicePoint, I can probably access everybody's records that are in here today, including social security numbers, maiden name, etc.

**Parrell Grossman:** Yes, if you are a customer of that company, you can access that information, unless for any reason that information would be protected or prohibited. I think if the information is gathered by ChoicePoint, that information is sold by ChoicePoint. I should mention for the committee's benefit, that ChoicePoint also gathers many public records that are already available, just not in one convenient spot, they might already have all the records regarding divorces, bankruptcies, maybe even in some cases, criminal records. They have it now gathered, and they bundled it together in a very neat package where identity thieves, or anyone, can now access all of that information about me, as a consumer, and I think that presents greater harm than the fact that the information already exists in various public locations.

**Chairman DeKrey:** Thank you. Further testimony in support of SB 2251. Testimony in opposition. We will close the hearing.

Page 10  
House Judiciary Committee  
Bill/Resolution Number SB 2251  
Hearing Date 3/7/05

(Reopened in the afternoon session).

**Chairman DeKrey:** What are the committee's wishes in regard to SB 2251.

**Representative Delmore:** I move that we put an emergency clause on SB 2251.

**Representative Meyer:** Seconded.

**Chairman DeKrey:** Motion carried.

**Representative Maragos:** I move the Attorney General's amendments.

**Representative Delmore:** Seconded.

**Chairman DeKrey:** Motion carried.

**Representative Koppelman:** I move a Do Pass as amended.

**Representative Maragos:** Seconded.

14 YES 0 NO 0 ABSENT      DO PASS AS AMENDED      CARRIER: Rep. Delmore

Date: 3/7/05  
Roll Call Vote #: 1

2005 HOUSE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 2251

HOUSE JUDICIARY COMMITTEE

☐ Check here for Conference Committee

Legislative Council Amendment Number \_\_\_\_\_

Action Taken Do Pass as Amended

Motion Made By Rep. Koppelman Seconded By Rep. Maragos

Representatives	Yes	No	Representatives	Yes	No
Chairman DeKrey	✓		Representative Delmore	✓	
Representative Maragos	✓		Representative Meyer	✓	
Representative Bernstein	✓		Representative Onstad	✓	
Representative Boehning	✓		Representative Zaiser	✓	
Representative Charging	✓				
Representative Galvin	✓				
Representative Kingsbury	✓				
Representative Klemin	✓				
Representative Koppelman	✓				
Representative Kretschmar	✓				

Total (Yes) 14 No 0

Absent 0

Floor Assignment Rep. Delmore

If the vote is on an amendment, briefly indicate intent:

**REPORT OF STANDING COMMITTEE**

SB 2251, as engrossed: Judiciary Committee (Rep. DeKrey, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (14 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). Engrossed SB 2251 was placed on the Sixth order on the calendar.

Page 1, line 1, after "Act" insert "to create and enact chapter 51-30 of the North Dakota Century Code, relating to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form;"

Page 1, line 4, remove "and" and after "penalty" insert "; and to declare an emergency"

Page 1, line 15, overstrike "39-04-14" and insert immediately thereafter "39-06-14"

Page 1, line 24, after "individual" insert ", living or deceased,"

Page 2, after line 27, insert:

**"SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

51-30-01. Definitions.In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security system" means unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a person. Good-faith acquisition of personal information for the purposes of the person maintaining the information by an employee or agent of the person is not a breach of the security of the system, provided that the personal information is not used or subject to further disclosure.
2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when either the name or the data elements are not encrypted:
  - (1) The individual's social security number;
  - (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
  - (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
  - (4) The individual's financial institution account number, credit card number, or debit card number;
  - (5) The individual's date of birth;
  - (6) The maiden name of the individual's mother; or
  - (7) An identification number assigned to the individual by the individual's employer.

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

51-30-02. Notice to consumers. Any person that conducts business in North Dakota, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

51-30-03. Notice to owner or licensee of personal information. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

51-30-04. Delayed notice. The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

51-30-05. Method of notice. Notice under this chapter may be provided by one of the following methods:

1. Written notice;
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of the United States Code; or
3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice includes:
  - a. E-mail notice;
  - b. Conspicuous posting of the notice on the person's web site page; or
  - c. Notification to major statewide media.

51-30-06. Alternate compliance. Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of section 51-30-05, is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system.

51-30-07. Enforcement - Powers - Remedies - Penalties. The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the

powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

**SECTION 4. EMERGENCY.** This Act is declared to be an emergency measure."

Renumber accordingly

2005 SENATE JUDICIARY

CONFERENCE COMMITTEE

SB 2251

}



2005 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. HB 2251

Senate Judiciary Committee

■ Conference Committee

Hearing Date March 28, 2005

Tape Number	Side A	Side B	Meter #
1	X		0.0 - 2550
Committee Clerk Signature <i>Maria L. Salvey</i>			

CONFERENCE COMMITTEE

Minutes: Relating to the use of personal identifying info involving conduct outside of ND.

**Senator John Syverson**, Chairman called the conference committee to order. All Senators and representatives were present. The hearing opened with the following: The Senate did not concur do to the desire to add some additional amendments to the bill. They are in agreement with the house amendments.

**Senator Syverson** introduced an amendment to presented by **Perrell D. Grossman**, Dir.

Consumer Protection. These amendments are presented on the behalf of the Attorney Generals office and Joel Gilbertson on behalf of his clients. These amendments are a result of the "Choice Point" scandal. Perrell reviewed the amendments. Discussed the process of why the bill was in the conference committee and being in compliance with the Federal Regulation or FACT Law- Att. #1 with the "mockup" The committee discusses his set amendments.

**Senator Syverson** questioned page 3, line 8 is this what would happen if a banks laptop was stolen. The amendments are consistent with other law; CA, MN and IN. Discussion of the removal of date of birth and electronic signature. Discussion of the University's security of its systems. In items A-J we could add perhaps 4 or more items to this section. We will review this for the next section.

**Senator Triplett** stated that on SB 2249 regarding receipts that have ID information that showed not have confidential information be a class B misdemeanor. How will this effect the bill.

**Senator Syverson** thought at first he was concerned that these amendments should have hearings unto themselves but after this review they are germane to what is already in the bill

**Senator John Syverson**, Chairman recessed the Hearing

2005 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. HB 2251

Senate Judiciary Committee

■ Conference Committee

Hearing Date March 30, 2005

Tape Number	Side A	Side B	Meter #
1	X		970 - End
Committee Clerk Signature <i>Maria L. Salberg</i>			

Minutes: Relating to the use of personal identifying info involving conduct outside of ND.

**Senator John (Jack) T. Traynor**, Chairman called the Judiciary committee to order. All Senators were present. The hearing opened with the following testimony:

**Testimony In Support of the Bill:**

**Senator Syverson** introduced an amendment to presented by **Perrell D. Grossman**, Dir.

Consumer Protection Attorney Generals office. - Att. #1 with the "mockup" of Att. #2.

The committee discusses his second set amendments. and mockup #2 that would address Rep.

**Delmores** concern and Chairman Syverson's concern.

**Rep. Maragos** said that we should get rid of the first amendment and mock up #1 so to not be confused.

**Rep. Delmore** still questioned page 3, line 18. We added the language "a combination of any required...." You feel that just having the credit card number is not a breach? **Mr. Grossman** responded (meter 1620) if a pass word or code is required to access the account then it is not

necessary, then there is no or minimal risk to a consumer. If it is not encrypted than it would constitute a security breach and it would trigger notification to card holder.

**Rep. Marago** asked we had restored date of birth and ID numbers back into the bill? Yes.

Senator Triplett asked for a background of FACT. (meter 1750)

**Marlyn Foss**, ND Bankers Assoc. Gave an overview of FACT.

The committee discussed in detail corporate ID numbers, electronic signature, credit card security (with numbers on back of card)

The committee discussed in detail how accounts are accessed. **Senator Triplett** said that it would upset her greatly if a bank would give a disk to the child support agency saying that they were customers of the bank. This legislation is modeled after MN, CA and several other states.

**Senator Hacker** talked how easy it is to get a credit card number, the difficulty is in the numbers on the back of the card and the expiration date. Rep. Maragos questioned the elimination of sub. 7 line 21. (meter 2321). **Rep. Margos** asked what "primary ID's are; Social Security number, Bank numbers, date of birth, and mothers maiden name. Discussed great concern for company ID numbers and referred to the "State" depositing system..

**Senator John Syverson**, Chairman closed the Hearing

2005 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2251

Senate Judiciary Committee

■ Conference Committee

Hearing Date April 1, 2005 and April 7, 2005

Tape Number	Side A	Side B	Meter #
1	X		0.0 - End
Committee Clerk Signature <i>Maria L. Solberg</i>			

CONFERENCE COMMITTEE

April 1, 2005

Minutes: Relating to the use of personal identifying info involving conduct outside of ND.

**Senator Syverson**, Chairman called the Judiciary committee to order. All Senators and Representatives were present. The hearing opened with the following:

Opened with a review of work from the previous meeting with **Perrell Grossman**, Attorney General's office introduces the April 4 amendment and reviewed Employee ID #- Att. #1

Discussed additional amendments that would not take him long to do. If the committee so desires I can put it together. Also discussed the Emergency Clause effective date of June 1.

The changes from the first proposed amendments are page 3, line 4 - changing it to A 1-8 what would change we would add a section 8 - Electronic Signature and Employers ID number. and the additional language to put an Emergency Clause. and Financial Institutions already having there procedures in place via Federal Law.

**Senator Triplett** asked **Mr. Grossman** to put this all together in a clean mockup.

**Senator Syverson**, Chairman was in approval of this as was the committee. Committee complemented **Mr. Grossman** on his excellent work.

Meeting to be rescheduled for the following Monday.

**Senator John Syverson**, Chairman closed the Hearing

#### CONFERENCE COMMITTEE

April 7, 2005

Minutes: Relating to the use of personal identifying info involving conduct outside of ND.

**Senator Syverson**, Chairman called the Judiciary committee to order. All Senators and Representatives were present. The hearing opened with the following: (meter 950)

**Mr. Grossman** introduced the final set of completed mock up - Att. #1a and Amendment - Att.

#1. He reviewed the final amendments with the committee

**Rep. Maragos** made the motion that the house recedes from its amendments and further amends and it is seconded by **Rep. Delmore** seconds the motion and all members are in favor. Motion passes.

**Senator Triplett** made the motion to Do pass as Amended and seconded by **Rep. Maragos**. All members were in favor and the motion passes.

**Senator John Syverson**, Chairman closed the Hearing

Date: 4/7/05  
Roll Call Vote #:

2005 SENATE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 2251

Senate Judiciary Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number \_\_\_\_\_

Action Taken House Recedes + Further Amends 1a

Motion Made By Rep Maragos Seconded By Rep Delmore

Senators	Yes	No	<del>Senators</del>	Yes	No
Senator Syverson - Chair	✓		Rep. Maragos (1)	✓	
Senator Hacker	✓		Rep. Charging	✓	
Senator Triplett	✓		Rep. Delmore (2)	✓	

Total (Yes) 6 ~~Click here to type Yes Vote~~ No 6 ~~Click here to type No Vote~~

Absent \_\_\_\_\_

Floor Assignment Click here to type Floor Assignment

If the vote is on an amendment, briefly indicate intent:

Date: 4/17/03  
Roll Call Vote #: 2

**2005 SENATE STANDING COMMITTEE ROLL CALL VOTES**  
**BILL/RESOLUTION NO. SB 2251**

Senate Judiciary Committee

☐ Check here for Conference Committee

Legislative Council Amendment Number \_\_\_\_\_

Action Taken Do Pass AS Amendment April 4th

Motion Made By Sen Triplett Seconded By Rep Maragos

Senators	Yes	No	<del>Rep</del> <del>Senators</del>	Yes	No
Senator Syverson - Chair	✓		Rep. Maragos (2)	✓	
Senator Hacker	✓		Rep. Charging	✓	
Senator Triplett (1)	✓		Rep. Delmore	✓	

Total (Yes) 6 Click here to type Yes Vote No 0 Click here to type No Vote

Absent \_\_\_\_\_

Floor Assignment Click here to type Floor Assignment

If the vote is on an amendment, briefly indicate intent:



**REPORT OF CONFERENCE COMMITTEE**

**SB 2251, as engrossed:** Your conference committee (Sens. Syverson, Hacker, Triplett and Reps. Maragos, Charging, Delmore) recommends that the **HOUSE RECEDE** from the House amendments on SJ pages 786-787, adopt amendments as follows, and place SB 2251 on the Seventh order:

That the House recede from its amendments as printed on pages 786 and 787 of the Senate Journal and pages 944 and 945 of the House Journal and that Engrossed Senate Bill No. 2251 be amended as follows:

Page 1, line 1, after "Act" insert "to create and enact chapter 51-30 of the North Dakota Century Code, relating to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form;"

Page 1, line 4, remove "and" and after "penalty" insert "; to provide an effective date; and to declare an emergency"

Page 1, line 15, overstrike "39-04-14" and insert immediately thereafter "39-06-14"

Page 1, line 20, overstrike "or"

Page 1, line 21, after "institution" insert "; or"

Page 1, line 24, after "individual" insert ", living or deceased."

Page 2, after line 27, insert:

**"SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

51-30-01. Definitions. In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or data bases unreadable or unusable. Good-faith acquisition of personal information by an employee or agent of the person is not a breach of the security of the system, if the personal information is not used or subject to further unauthorized disclosure.
2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:
  - (1) The individual's social security number;
  - (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
  - (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
  - (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required

security code, access code or password that would permit access to an individual's financial accounts;

- (5) The individual's date of birth;
- (6) The maiden name of the individual's mother;
- (7) An identification number assigned to the individual by the individual's employer; or
- (8) The individual's digitized or other electronic signature.

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

51-30-02. Notice to consumers. Any person that conducts business in this state, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

51-30-03. Notice to owner or licensee of personal information. Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

51-30-04. Delayed notice. The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

51-30-05. Method of notice. Notice under this chapter may be provided by one of the following methods:

1. Written notice;
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; or
3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice consists of the following:
  - a. E-mail notice when the person has an e-mail address for the subject persons;

- b. Conspicuous posting of the notice on the person's web site page, if the person maintains one; and
- c. Notification to major statewide media.

51-30-06. Alternate compliance. Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company, or credit union that is subject to, examined for, and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with this chapter.

51-30-07. Enforcement - Powers - Remedies - Penalties. The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

**SECTION 4. EFFECTIVE DATE.** This Act becomes effective on June 1, 2005.

**SECTION 5. EMERGENCY.** This Act is declared to be an emergency measure."

Renumber accordingly

Engrossed SB 2251 was placed on the Seventh order of business on the calendar.

2005 TESTIMONY

SB 2251

**SENATE BILL NO. 2251**

*Attorney General*

This legislation enhances the criminal penalties for Identity Theft. ID Theft would be a class B felony unless the value of the property is \$1,000 or less, in which case it would be a class C felony. A second or subsequent offense is a class A felony.

ID Theft across the country continues to grow at an alarming rate. According to the New York Times more than 27 million Americans have been victims of Identity Theft in the last five years. Consumers have reported nearly \$5 billion in out of pocket expenses.

According to one source, this year more than 500,000 Americans will be robbed of their identities with more than \$4 billion stolen in their names.

North Dakotans are not immune from ID Theft. ID Theft in North Dakota is increasing as it is across the country. Each month my office processes ID Theft reports and issues Affidavits of Identity Theft for several victims.

This crime has horrendous consequences for its victims. The Identity Theft Resource Center calculates that victims spend an average of 600 hundred hours recovering from this crime, often over a period of years. Three years ago the average was 175-200 hours, an increase of more than 300 percent. The business community loses between \$40,000-\$92,000 per name in fraudulent charges.

It is time to hold these ID thieves responsible for the consequences and seriousness of their actions that devastate the lives of their victims who often are unable to obtain financing for home loans, obtain employment, and sometimes are even arrested for crimes committed in their names by the ID thieves.

Attorneys General across the country are all taking notice of this problem as their states grapple with Identity Theft and enact stricter legislation, as well as enhancing protections for ID Theft victims.

This legislation will send a clear message to ID thieves that North Dakota is serious.

Section 2 addresses jurisdiction and will ensure the ability to prosecute the crime in North Dakota for our victims even when the crime or part of it occurs outside the state. Many states are overwhelmed and unable, or maybe even unwilling, to prosecute all the ID Thefts in their states. We could prosecute in North Dakota those ID thefts originating outside the state. The legislation also includes changes permitting prosecution in one county for ID thefts that occur in multiple counties.

SENATE JUDICIARY COMMITTEE  
JOHN T. TRAYNOR, CHAIRMAN  
FEBRUARY 1, 2005

TESTIMONY BY  
PARRELL D. GROSSMAN  
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL  
IN SUPPORT OF  
SENATE BILL NO. 2251

Mr. Chairman and members of the Senate Judiciary Committee. I am Parrell Grossman, Director of the Consumer Protection and Antitrust Division of the Attorney General's Office. The Attorney General and the Consumer Protection Division support Senate Bill No. 2251.

The Attorney General supports this legislation because it addresses the fast growing crime of Identity Theft. It enhances the criminal penalties for Identity Theft in recognition of the very serious nature of this crime. It increases the penalties from a class C felony to a class A felony, unless the value of the money, goods, or services is \$1,000 or less. A second or subsequent offense is a class A felony.

This legislation is necessary because Id Theft is growing throughout the country at an alarming, enormous rate. According to the New York Times more than 27 million Americans have been victims of Identity Theft in the last five years, and consumers have reported more than \$5 billion dollars in out-of-pocket expenses. According to CBSnews.com, "This year alone more than 500,000 Americans will be robbed of their identities ...with more than \$4 billion dollars stolen in their names."

This crime continues to increase in North Dakota. Because ID thefts are reported to various law enforcement agencies in this state, it is difficult to accurately estimate the number of ID Theft victims in North Dakota. Since the Attorney General started accepting ID Theft Reports and issuing ID Theft Affidavits in September, we have experienced Id Theft reports of several each month. The Attorney General works with these victims to ensure they take steps to report the theft and start repairing the damage.

The Us Department of Justice reported in one notorious case of ID Theft that the criminal incurred over \$100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and hand guns all in the victim's name all the while calling the victim to taunt him.

CBSnews.com reported that a convicted ID thief in Denver, Colorado stated that, "on a good day I could make \$5,000 in cash and another \$7,000 to \$8,000 in merchandise."

ID Theft is a very serious crime with very serious consequences for the victims. According to a report from the Identity Theft Resource Center victims now spend an average of 600 hundred hours recovering from this crime, often over a period of years. Based on 600 hours times the indicated victim's wages, this equals nearly \$16,000 in lost potential or realized income. The Center also reports that today the business community loses between \$40,000 and \$92,000 per name in fraudulent charges, based on fraud losses incurred by surveyed victims.

Victims of ID Theft can suffer the loss of excellent credit histories built over a lifetime of responsible decisions. They can lose employment opportunities when a potential employer does a credit check. They can be denied home loans when trying to purchase their "dream homes." They can even be arrested for crimes the ID Thief committed in their names.

This legislation, by enhancing penalties seeks to hold ID thieves accountable for their actions, with possible punishments that fit the harsh crimes.

In addition, the proposed changes ensure that ID thefts occurring in multiple counties can be prosecuted in one county.

Section 2 of this bill addresses jurisdictional issues and provides authority to prosecute ID thieves who, from locations outside North Dakota, steal from North Dakota victims. Some jurisdictions are overwhelmed with other crimes, or won't even take police reports. North Dakota courts will have jurisdiction and victims will have a jurisdiction that will prosecute the crimes for North Dakota victims.

For these reasons, the Attorney General and his Consumer Protection Division urge this committee to give Senate Bill 2251 a "do pass" recommendation.

Thank you for your time and consideration. I will try and answer any questions.

**Testimony****Senate Bill 2251****Senate Judiciary Committee****February 1, 2005; 10 a.m.****North Dakota Department of Health**

Good morning, Chairman Traynor and members of the Senate Judiciary Committee. My name is Darin Meschke, and I am the state registrar and director of the Division of Vital Records for the North Dakota Department of Health. I am here to request an amendment to Senate Bill 2251 adding an individual's birth, death or marriage certificate to the list of personal identifying information in lines 11-21.

Birth, death and marriage certificates are three vital event documents that can be used in the identity theft process and in other fraudulent activities. These three documents contain key pieces of information about an individual and are widely accepted as identity documents by businesses and government agencies to obtain credit or services.

A person's birth certificate is required to obtain a North Dakota driver's license and a social security number – both of which are necessary to establish identity. In addition, death and marriage certificates may be used in the identity theft process and are sometimes used to illegally obtain money, goods or services in someone else's name. Birth, death and marriage certificates should carry the same penalty for unlawful use as the information already listed in Senate Bill 2251.

This concludes my testimony. I am happy to answer any questions you may have.



Att 4

PROPOSED AMENDMENTS TO SENATE BILL NO. 2251  
SENATE JUDICIARY COMMITTEE COMMITTEE  
JOHN T. TRAYNOR, CHAIRMAN  
FEBRUARY 1, 2005

PRESENTED BY  
DARIN J. MESCHKE, DIRECTOR  
DIVISION OF VITAL RECORDS  
ND DEPARTMENT OF HEALTH

Page 1, after line 21, insert:

"j. An individual's birth, death or marriage certificate.

Renumber accordingly

# IDENTITY

Identity theft is a crime. Under federal law you have certain rights, but you must take the following steps to assert these rights:

## 1. File a report with your local law enforcement agency.

Ask for a copy of the police report, or the complaint number.

## 2. File a report with the Attorney General's office.

The Attorney General's office is North Dakota's clearing house for identity theft. We will provide you with the information and forms you need to document the theft and restore your credit.

## 3. Report the fraud to the credit bureaus.

Request a "fraud alert" be placed in your file, to stop creditors opening any new accounts or changing your existing ones. Always follow up with a letter. Order a free credit report from each credit bureau, so you can check for other fraudulent accounts.

## 4. Close the accounts that have been tampered with or opened fraudulently.

Ask to speak with someone in the security or fraud department of each creditor, and follow up with a letter. "Creditor" can include credit card and telephone companies, utilities, banks and other lenders.

Contact the three credit bureaus:

	EQUIFAX	EXPERIAN	TRANS UNION
Mailing Address	PO Box 740241 Atlanta GA 30374-0241	PO Box 9530 Allen TX 75013	PO Box 6790 Fullerton CA 92634
Website	www.equifax.com	www.experia.n.com	www.transunion.com
Report Fraud	800-525-6285	888-397-3742	800-680-7289

Stop telemarketing calls—Register on the Do Not Call list at 1-888-382-1222.

Stop junk mail—Get the form free from the Consumer Protection Division.



OFFICE OF ATTORNEY GENERAL  
Wayne Stenehjem, Attorney General

For information or to file a report, contact:

Consumer Protection Division

Local: 701-328-3404

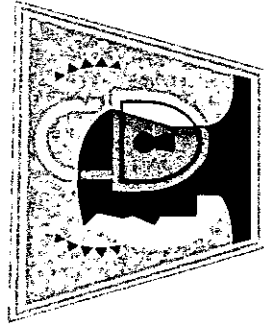
Toll Free 1-800-472-2600

TTY: 1-800-366-6888

e-mail: [cpat@state.nd.us](mailto:cpat@state.nd.us)

[www.ag.state.nd.us](http://www.ag.state.nd.us)

# Identity Theft



The act of stealing your good name to commit fraud.

*Most people never think about the day-to-day activities that expose personal information to identity thieves - until it's too late.*

Besides basic information such as name and address, identity thieves look for dates of birth, a driver's license, social security number (SSN), credit card and bank account numbers, and telephone calling cards.

### Identity Thieves:

- look through your trash for canceled checks, bank statements and pre-approved credit card applications;
- use technology to steal your personal and financial information;
- pretend to be company officials, to trick you into revealing personal information.

The thief uses your information to hijack existing accounts and open new accounts in your name. When your credit is gone, the thief moves on—leaving you to sort out the devastating consequences.



The theft of your identity can leave you with a poor credit rating and a ruined reputation that may take **months or even years** to correct. Meanwhile, you may be denied a job, a new car, or even a new home.



*The average bank robber steals \$2,500. The average loss to identity theft is \$50,000.*

*These few simple steps can keep your information safe:*

- ✓ **Don't** use your SSN as your driver's license number. Your SSN accesses your credit history, criminal, medical and school records, credit cards, bank accounts, financial records and social security benefits.



- ✓ **Never** give out your credit card number or other personal information over the telephone unless you **initiated** the call **and** you are sure it is a reputable company.

- ✓ **Remove** "extra" information—such as your SSN, home phone, and date of birth—from your checks. A merchant cannot require you to write your SSN on a check.

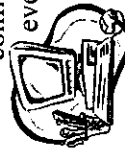


- ✓ **Shred** any papers, documents or statements that contain account or personal information before throwing them away. Shred junk mail, and credit card applications, too.



- ✓ **Check** your bank and credit card statements, cancelled checks, phone and utility bills as soon as you get them. Report any discrepancies immediately.

- ✓ **Never** respond to an e-mail asking you to confirm or verify account information, even if it looks "official." Instead, call the customer service number listed on the company's billing statement to check the account.



- ✓ **Shop** online only with reputable businesses, and make sure the site is **secure** before providing credit card information.



- ✓ **Provide** only the necessary information on warranty and registration forms—don't answer marketing or survey questions, and don't respond to phone surveys.

- ✓ **Call** the National Credit Bureaus, toll-free at 1-888-567-8688 to **stop** receiving unsolicited credit card applications. You will have to provide your SSN.

*Your social security number is your most valuable asset. It identifies YOU.*

HOUSE JUDICIARY COMMITTEE  
DUANE DEKREY, CHAIRMAN  
MARCH 7, 2005

TESTIMONY BY  
PARRELL D. GROSSMAN  
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL  
IN SUPPORT OF  
ENGROSSED SENATE BILL NO. 2251

Mr. Chairman and members of the House Judiciary Committee. I am Parrell Grossman, Director of the Consumer Protection and Antitrust Division of the Attorney General's Office. The Attorney General and the Consumer Protection Division support Engrossed Senate Bill No. 2251.

The Attorney General supports this legislation because it addresses the fast growing crime of Identity Theft. It enhances the criminal penalties for Identity Theft in recognition of the very serious nature of this crime. It increases the penalties from a class C felony to a class A felony, unless the value of the money, goods, or services is \$1,000 or less. A second or subsequent offense is a class A felony.

This legislation is necessary because ID Theft is growing throughout the country at an alarming, enormous rate. According to the New York Times more than 27 million Americans have been victims of Identity Theft in the last five years, and consumers have reported more than \$5 billion dollars in out-of-pocket expenses. According to CBSnews.com, "This year alone more than 500,000 Americans will be robbed of their identities ...with more than \$4 billion dollars stolen in their names."

This crime continues to increase in North Dakota. Because ID thefts are reported to various law enforcement agencies in this state, it is difficult to accurately estimate the number of ID Theft victims in North Dakota. Since the Attorney General started accepting ID Theft Reports and issuing ID Theft Affidavits in September, we have experienced Id Theft reports of several each month. The Attorney General works with these victims to ensure they take steps to report the theft and start repairing the damage.

The Us Department of Justice reported in one notorious case of ID Theft that the criminal incurred over \$100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and hand guns all in the victim's name all the while calling the victim to taunt him.

CBSnews.com reported that a convicted ID thief in Denver, Colorado stated that, "on a good day I could make \$5,000 in cash and another \$7,000 to \$8,000 in merchandise."

ID Theft is a very serious crime with very serious consequences for the victims. According to a report from the Identity Theft Resource Center victims now spend an average of 600 hundred hours recovering from this crime, often over a period of years. Based on 600 hours times the indicated victim's wages, this equals nearly \$16,000 in lost potential or realized income. The Center also reports that today the business community loses between \$40,000 and \$92,000 per name in fraudulent charges, based on fraud losses incurred by surveyed victims.

ID theft complaints comprised 39% of the 635,000 total fraud complaints filed with the FTC in 2004.

Victims of ID Theft can suffer the loss of excellent credit histories built over a lifetime of responsible decisions. They can lose employment opportunities when a potential employer does a credit check. They can be denied home loans when trying to purchase their "dream homes." They can even be arrested for crimes the ID Thief committed in their names.

This legislation, by enhancing penalties seeks to hold ID thieves accountable for their actions, with possible punishments that fit the harsh crimes.

In addition, the proposed changes ensure that ID thefts occurring in multiple counties can be prosecuted in one county.

Section 2 of this bill addresses jurisdictional issues and provides authority to prosecute ID thieves who, from locations outside North Dakota, steal from North Dakota victims. Some jurisdictions are overwhelmed with other crimes, or won't even take police reports. North Dakota courts will have jurisdiction and victims will have a jurisdiction that will prosecute the crimes for North Dakota victims.

The Attorney General is proposing some amendments to Engrossed Senate Bill 2251.

First on page 1, line 15 replace "39-04-14" with 39-06-14." The current reference to a driver's license number assigned by the department of transportation under section 39-04-14 is incorrect. That section addresses motor vehicle registrations and has nothing to do with the assignment of driver's license numbers. Section 39-06-14 is the section that provides for the assignment of driver's license numbers.

Next, we propose a change on line 24 to insert language from House Bill 1211, sponsored by, among others, Representative Delmore, Chairman Dekrey, and Representative Maragos. The Senate has amended House Bill 1211 to mirror SB 2251. However, that provision is not currently in SB 2251. It is an important and significant change and it should be incorporated in SB 2251, too.

Finally, the proposed amendments include what might be considered the "Security Breach Disclosure Act," if this legislature used short titles. This proposed legislation addresses the disclosure of breach in security by businesses maintaining computerized data containing personal information. These companies, among other names, are referred to as "data warehousers" and "information brokers."

ChoicePoint of Alpharetta, Georgia is one of the nation's largest information brokers. Its databases contain 19 billion records. In October 2004 the company discovered a breach of its security. Identity thieves, posing as check-cashing companies or debt-collection firms, set up approximately 50 fraudulent business accounts and gained access to ChoicePoint's consumer data. This has been characterized as a "low-tech" theft and it did not involve a high-tech

hijacking or hacking of computer information. The ID thieves stole accessed Social Security Numbers, credit reports, criminal records, and other sensitive data.

Initial information indicated it appeared 145,000 consumers were affected by the security breach. ChoicePoint apparently has admitted even more consumers than first thought could be victims. The Los Angeles, California investigation task force leader believes at least 700 consumers were defrauded, and believes the number of people vulnerable to Identity theft could reach 500,000.

ChoicePoint delayed notifying potential victims due to a law enforcement request that such notification would compromise its investigation. The company announced plans to notify California citizens that their personal information may have been compromised. California has a law requiring consumer notification of security breaches. On February 16, 2005, Attorney General Stenehjem and attorneys general from 18 other states requested by letter that ChoicePoint take immediate corrective action to notify all citizens of these states who may have been affected by this security breach. ChoicePoint agreed to do so. We have been informed that letters have been sent to 137 affected consumers in North Dakota. The Attorney General and I, as well as a Consumer Protection Investigator have spent many hours reviewing this matter, and addressing inquiries from worried North Dakota consumers. Our task is not yet completed.

The media recently reported that ChoicePoint had been the victim of a similar theft in 2002. Two individuals using a real estate license and driver's license for identification, opened ChoicePoint accounts and gained access to at least 7,000 consumers and reportedly purchases over \$1 million dollars in merchandise using these stolen identities. A company spokesman did not know if the problem was publicly disclosed in 2002.

In 2003, Acxiom, another personal-information clearinghouse, suffered a security breach when two individuals stole the records of thousands of consumers.

Minnesota, New York, Texas, and Georgia are among states considering laws that mirror California's security breach law, which requires companies notify residents if their personal information is compromised. The Attorney General would like the North Dakota legislature to pass a law at this time requiring security breach disclosures to our North Dakota residents.

For these reasons, the Attorney General and his Consumer Protection Division urge this committee to adopt the Attorney General's proposed amendments to Engrossed Senate Bill 2251 and give Engrossed Senate Bill 2251 a "do pass" recommendation.

Thank you for your time and consideration.

PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2251  
HOUSE JUDICIARY COMMITTEE  
DUANE DEKREY, CHAIRMAN  
MARCH 7, 2005

PRESENTED BY  
PARRELL D. GROSSMAN, DIRECTOR  
CONSUMER PROTECTION & ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL

Page 1, line 1, after "Act" insert "to create and enact chapter 51-30 of the North Dakota Century Code relating to consumer protection requiring disclosure to consumers of a breach in Security by businesses maintaining personal information in electronic form;"

Page 1, line 15, replace "39-04-14" with "39-06-14"

Page 1, line 24, after "individual" insert ", living or deceased,"

Page 2, after line 27, insert:

**"SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

**51-30-01. Definitions.** In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further disclosure.
2. a. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) social security number; (2) operator's license number assigned to an individual by the department of transportation under section 39-06-14; (3) nondriver color photo identification card number assigned to an individual by the department of transportation pursuant to section 39-06-03.1; (4) financial institution account number, credit card number, or debit card number; (5) date of birth; (6) maiden name of the individual's mother; or (7) an identification number assigned to the individual by the individual's employer.
- b. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

**51-30-02. Notice to consumers.** Any person or business that conducts business in North Dakota, and that owns or licenses computerized data that includes personal

information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of North Dakota whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and restore the integrity of the data system.

**51-30-03. Notice to owner or licensee of personal information.** Any person or business that maintains computerized data that includes personal information that the person or business does not own shall the notify the owner or licensee of the information or breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

**51-30-04. Delayed notice.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter shall be made after the law enforcement agency determines that it will not compromise the investigation.

**51-30-05. Method of notice.** Notice under this chapter may be provided by one of the following methods:

1. Written notice.
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of the United States Code.
3. Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:
  - a. E-mail notice when the person or business has an e-mail address for the subject persons.
  - b. Conspicuous posting of the notice on the web site page of the person or business, if the person or business maintains one.
  - c. Notification to major statewide media.

**51-30-06. Alternate compliance.** Notwithstanding section 51-30-05, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of section 51-30-05, shall be deemed to be in compliance with the notification requirements of this chapter if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.



**51-30-07. Enforcement – Powers – Remedies - Penalties.** The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

Renumber accordingly.

HH #1

THIRD PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2251  
(FIRST ENGROSSMENT WITH HOUSE AMENDMENTS)  
CONFERENCE COMMITTEE  
JOHN O. SYVERSON, CHAIRMAN

PRESENTED BY  
PARRELL D. GROSSMAN, DIRECTOR  
CONSUMER PROTECTION & ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL  
APRIL 4, 2005

Page 1, line 6, after "penalty;" insert "to provide an effective date;"

Page 3, line 4, replace "which compromises the security, confidentiality, or integrity of personal information maintained by the person or business" with "when access to the personal information described in subsections 51-30-01(2)(a)(1)-(8) has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable"

Page 3, line 6, remove "for the purposes of the person maintaining the information"

Page 3, line 8, after "further" insert "unauthorized"

Page 3, line 10, remove "either"

Page 3, line 11, replace "or" with "and"

Page 3, line 18, after "debit card number" insert "in combination with any required security code, access code or password that would permit access to an individual's financial accounts"

Page 3, line 20, remove "or"

Page 3, line 22, replace the period with "or;"

Page 3, after line 22, insert:

"(8)The individual's digitized or other electronic signature."

Page 4, line 16, after "7001" insert "of Title 15"

Page 4, line 21, replace "includes" with "shall consist of all of the following"

Page 4, line 22, after "notice" insert "when the person has an email address for the subject persons"

Page 4, line 23, after "page" insert ", if the person maintains one"

Page 4, line 23, replace "or" with "and"

Page 4, line 28, replace "section 51-30-05" with "this chapter"

Page 4, line 30, insert: "A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter."

Page 5, after line 6, insert:

"SECTION 4. Effective Date. This Act becomes effective on June 1, 2005."

Renumber accordingly

PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2251  
(FIRST ENGROSSMENT WITH HOUSE AMENDMENTS)  
CONFERENCE COMMITTEE  
JOHN O. SYVERSON, CHAIRMAN

PRESENTED BY  
PARRELL D. GROSSMAN, DIRECTOR  
CONSUMER PROTECTION & ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL

Page 3, line 6, remove "for the purposes of the person maintaining the information"

Page 3, line 8, after "further" insert "unauthorized"

Page 3, line 8, after "disclosure" insert: "Unauthorized acquisition of a portable electronic device on which personal information is stored is not a breach of the system when access to the personal information or the device is protected by a password that has not been disclosed, or by another security measure designed to protect against unauthorized access."

Page 3, line 10, remove "either"

Page 3, line 11, replace "or" with "and"

Page 3, line 18, after "debit card number" insert "in combination with any required security code, access code or password that would permit access to an individual's financial accounts"

Page 3, remove line 19

Page 3, remove lines 21 and 22

Page 4, line 16, after "7001" insert "of Title 15"

Page 4, line 21, replace "includes" with "shall consist of all of the following"

Page 4, line 22, after "notice" insert "when the person has an email address for the subject persons"

Page 4, line 23, after "page" insert ", if the person maintains one"

Page 4, line 23, replace "or" with "and"

Page 4, line 28, replace "section 51-30-05" with "this chapter"

Page 4, line 30, insert: "A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter."

Renumber accordingly

4/7 AH 1a

SENATE BILL 2251  
(April 4, 2005 Mock-Up)

A BILL for an Act to create and enact chapter 51-30 of the North Dakota Century Code, relating to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; to amend and reenact sections 12.1-23-11 and 12.1-23-12 of the North Dakota Century Code, relating to the unauthorized use of personal identifying information, penalties, and prosecution of offenses in multiple counties; jurisdiction in offenses involving conduct outside this state; to provide a penalty; to provide an effective date; and to declare an emergency.

**BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

**SECTION 1. AMENDMENT.** Section 12.1-23-11 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-11. Unauthorized use of personal identifying information - Penalty.**

1. As used in this section, "personal identifying information" means any of the following information:

- a. An individual's name;
- b. An individual's address;
- c. An individual's telephone number;
- d. The distinguishing operator's license number assigned to an individual by the department of transportation under section 39-04-14 39-06-14;
- e. An individual's social security number;
- f. An individual's employer or place of employment;
- g. An identification number assigned to the individual by the individual's employer;
- h. The maiden name of the individual's mother; or
- i. The identifying number of a depository account in a financial institution.
- j. An individual's birth, death, or marriage certificate.

2. A person is guilty of a ~~class C felony~~ an offense if the person uses or attempts to use any personal identifying information of an individual, living or deceased, to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual and by representing that person is the individual or is acting with the authorization or consent of the individual. The offense is a class B felony if the credit, money, goods, services, or anything else of value exceeds one thousand dollars in value, otherwise the offense is a class C felony. A second or subsequent offense is a class A felony.

3. A violation of this section, of a law of another state, or of federal law that is equivalent to this section and which resulted in a plea or finding of guilt must be considered a prior offense. The prior offense must be alleged in the complaint, information, or indictment. The plea or finding of guilt for the prior offense must have occurred before the date of the commission of the offense or offenses charged in the complaint, information, or indictment.

4. A prosecution for a violation of this section must be commenced within six years after discovery by the victim of the offense of the facts constituting the violation.

5. When a person commits violations of this section in more than one county involving either one or more victims or the commission of acts constituting an element of the offense, the multiple offenses may be consolidated for commencement of prosecution in any county where one of the offenses was committed.

**SECTION 2. AMENDMENT.** Section 12.1-23-12 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-12. Jurisdiction - Conduct outside this state.** Notwithstanding section 29-03-01.1, a person who, while outside this state and by use of deception, obtains, deprives, or conspires, solicits, or attempts to obtain the property of a person within this state or to deprive such person of property is subject to prosecution under this chapter in the courts of this state. The Except as provided in section 12.1-23-11, the venue is in the county in which the victim resides or any other county in which any part of the crime occurred.

**SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

**51-30-01. Definitions.** In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security of the system" means unauthorized acquisition of computerized data when access to the personal information described in subsections 51-30-01.2.a.(1)-(8) has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable, that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information for the purposes of the person maintaining the information by an employee or agent of the person is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:

(1) The individual's social security number;

(2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;

(3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;

(4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code or password that would permit access to an individual's account;

(5) The individual's date of birth;

(6) The maiden name of the individual's mother;

(7) An identification number assigned to the individual by the individual's Employer; or

(8) The individual's digitized or other electronic signature.

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

**51-30-02. Notice to consumers.** Any person that conducts business in North Dakota, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

**51-30-03. Notice to owner or licensee of personal information.** Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

**51-30-04. Delayed notice.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

**51-30-05. Method of notice.** Notice under this chapter may be provided by one of the following methods:

1. Written notice;

2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code; or

3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice shall consist of all of the following:

- a. E-mail notice when the person has an email address for the subject persons;
- b. Conspicuous posting of the notice on the person's web site page, if the person maintains one; and
- c. Notification to major statewide media.

**51-30-06. Alternate compliance.** Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this chapter, is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter.

**51-30-07. Enforcement - Powers - Remedies - Penalties.** The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

**SECTION 4. Effective Date.** This Act becomes effective on June 1, 2005.

**SECTION 5. EMERGENCY.** This Act is declared to be an emergency measure.



AH #/b.

SENATE BILL 2251  
(Mock-Up 1)

A BILL for an Act to create and enact chapter 51-30 of the North Dakota Century Code, relating to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; to amend and reenact sections 12.1-23-11 and 12.1-23-12 of the North Dakota Century Code, relating to the unauthorized use of personal identifying information, penalties, and prosecution of offenses in multiple counties; jurisdiction in offenses involving conduct outside this state; to provide a penalty; and to declare an emergency.

**BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

**SECTION 1. AMENDMENT.** Section 12.1-23-11 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-11. Unauthorized use of personal identifying information - Penalty.**

1. As used in this section, "personal identifying information" means any of the following information:

- a. An individual's name;
- b. An individual's address;
- c. An individual's telephone number;
- d. The distinguishing operator's license number assigned to an individual by the department of transportation under section 39-04-14 39-06-14;
- e. An individual's social security number;
- f. An individual's employer or place of employment;
- g. An identification number assigned to the individual by the individual's employer;
- h. The maiden name of the individual's mother; or
- i. The identifying number of a depository account in a financial institution.
- j. An individual's birth, death, or marriage certificate.

2. A person is guilty of ~~a class C felony~~ an offense if the person uses or attempts to use any personal identifying information of an individual, living or deceased, to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual and by representing that person is the individual or is acting with the authorization or consent of the individual. The offense is a class B felony if the credit, money, goods, services, or anything else of value exceeds one thousand dollars in value, otherwise the offense is a class C felony. A second or subsequent offense is a class A felony.

3. A violation of this section, of a law of another state, or of federal law that is equivalent to this section and which resulted in a plea or finding of guilt must be considered a prior offense. The prior offense must be alleged in the complaint, information, or indictment. The plea or finding of guilt for the prior offense must have occurred before the date of the commission of the offense or offenses charged in the complaint, information, or indictment.

4. A prosecution for a violation of this section must be commenced within six years

after discovery by the victim of the offense of the facts constituting the violation.

5. When a person commits violations of this section in more than one county involving either one or more victims or the commission of acts constituting an element of the offense, the multiple offenses may be consolidated for commencement of prosecution in any county where one of the offenses was committed.

**SECTION 2. AMENDMENT.** Section 12.1-23-12 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-12. Jurisdiction - Conduct outside this state.** Notwithstanding section 29-03-01.1, a person who, while outside this state and by use of deception, obtains, deprives, or conspires, solicits, or attempts to obtain the property of a person within this state or to deprive such person of property is subject to prosecution under this chapter in the courts of this state. Except as provided in section 12.1-23-11, the venue is in the county in which the victim resides or any other county in which any part of the crime occurred.

**SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

**51-30-01. Definitions.** In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security system" means unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a person. Good-faith acquisition of personal information for the purposes of the person maintaining the information by an employee or agent of the person is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. Unauthorized acquisition of a portable electronic device on which personal information is stored is not a breach of the security system when access to the personal information or the device is protected by a password that has not been disclosed, or by another security measure designed to protect against unauthorized access.

2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when ~~either~~ the name ~~or~~ and the data elements are not encrypted:

- (1) The individual's social security number;
- (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
- (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
- (4) The individual's financial institution account number, credit card

number, or debit card number in combination with any required security code or password that would permit access to an individual's account;

(5) The individual's date of birth;

*keep*

(6) The maiden name of the individual's mother; or

(7) ~~An identification number assigned to the individual by the individual's employer.~~

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

**51-30-02. Notice to consumers.** Any person that conducts business in North Dakota, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

**51-30-03. Notice to owner or licensee of personal information.** Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

**51-30-04. Delayed notice.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

**51-30-05. Method of notice.** Notice under this chapter may be provided by one of the following methods:

1. Written notice;

2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code; or

3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice ~~includes~~ shall consist of all of the following:

- a. E-mail notice when the person has an email address for the subject persons;
- b. Conspicuous posting of the notice on the person's web site page, if the person maintains one; or and
- c. Notification to major statewide media.

**51-30-06. Alternate compliance.** Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of ~~section 51-30-05~~, this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter.

**51-30-07. Enforcement - Powers - Remedies - Penalties.** The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

**SECTION 4. EMERGENCY.** This Act is declared to be an emergency measure.

7

AH # 2a 3/30?

SECOND PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2251  
(FIRST ENGROSSMENT WITH HOUSE AMENDMENTS)  
CONFERENCE COMMITTEE  
JOHN O. SYVERSON, CHAIRMAN

PRESENTED BY  
PARRELL D. GROSSMAN, DIRECTOR  
CONSUMER PROTECTION & ANTITRUST DIVISION  
OFFICE OF ATTORNEY GENERAL

Page 3, line 4, replace "which compromises the security, confidentiality, or integrity of personal information maintained by the person or business" with "when access to the personal information described in subsections 51-30-01(2)(a)(1)-(7) has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable"

Page 3, line 6, remove "for the purposes of the person maintaining the information"

Page 3, line 8, after "further" insert "unauthorized"

Page 3, line 10, remove "either"

Page 3, line 11, replace "or" with "and"

Page 3, line 18, after "debit card number" insert "in combination with any required security code, access code or password that would permit access to an individual's financial accounts"

Page 3, remove line 21 and insert immediately thereafter "The individual's digitized or other electronic signature."

Page 3, remove line 22

Page 4, line 16, after "7001" insert "of Title 15"

Page 4, line 21, replace "includes" with "shall consist of all of the following"

Page 4, line 22, after "notice" insert "when the person has an email address for the subject persons"

Page 4, line 23, after "page" insert ", if the person maintains one"

Page 4, line 23, replace "or" with "and"

Page 4, line 28, replace "section 51-30-05" with "this chapter"

Page 4, line 30, insert: "A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter."

ATT # 2b

SENATE BILL 2251  
(Mock-Up 2)

A BILL for an Act to create and enact chapter 51-30 of the North Dakota Century Code, relating to requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; to amend and reenact sections 12.1-23-11 and 12.1-23-12 of the North Dakota Century Code, relating to the unauthorized use of personal identifying information, penalties, and prosecution of offenses in multiple counties; jurisdiction in offenses involving conduct outside this state; to provide a penalty; and to declare an emergency.

**BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

**SECTION 1. AMENDMENT.** Section 12.1-23-11 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-11. Unauthorized use of personal identifying information - Penalty.**

1. As used in this section, "personal identifying information" means any of the following information:

- a. An individual's name;
- b. An individual's address;
- c. An individual's telephone number;
- d. The distinguishing operator's license number assigned to an individual by the department of transportation under section 39-04-14 39-06-14;
- e. An individual's social security number;
- f. An individual's employer or place of employment;
- g. An identification number assigned to the individual by the individual's employer;
- h. The maiden name of the individual's mother; or
- i. The identifying number of a depository account in a financial institution.
- j. An individual's birth, death, or marriage certificate.

2. A person is guilty of a class ~~C~~ B felony an offense if the person uses or attempts to use any personal identifying information of an individual, living or deceased, to obtain credit, money, goods, services, or anything else of value without the authorization or consent of the individual and by representing that person is the individual or is acting with the authorization or consent of the individual. The offense is a class B felony if the credit, money, goods, services, or anything else of value exceeds one thousand dollars in value, otherwise the offense is a class C felony. A second or subsequent offense is a class A felony.

3. A violation of this section, of a law of another state, or of federal law that is equivalent to this section and which resulted in a plea or finding of guilt must be considered a prior offense. The prior offense must be alleged in the complaint, information, or indictment. The plea or finding of guilt for the prior offense must have occurred before the date of the commission of the offense or offenses charged in the complaint, information, or indictment.

4. A prosecution for a violation of this section must be commenced within six years after discovery by the victim of the offense of the facts constituting the violation.

5. When a person commits violations of this section in more than one county involving either one or more victims or the commission of acts constituting an element of the offense, the multiple offenses may be consolidated for commencement of prosecution in any county where one of the offenses was committed.

**SECTION 2. AMENDMENT.** Section 12.1-23-12 of the North Dakota Century Code is amended and reenacted as follows:

**12.1-23-12. Jurisdiction - Conduct outside this state.** Notwithstanding section 29-03-01.1, a person who, while outside this state and by use of deception, obtains, deprives, or conspires, solicits, or attempts to obtain the property of a person within this state or to deprive such person of property is subject to prosecution under this chapter in the courts of this state. Except as provided in section 12.1-23-11, the venue is in the county in which the victim resides or any other county in which any part of the crime occurred.

**SECTION 3.** Chapter 51-30 of the North Dakota Century Code is created and enacted as follows:

**51-30-01. Definitions.** In this chapter, unless the context or subject matter otherwise requires:

1. "Breach of the security of the system" means unauthorized acquisition of computerized data when access to the personal information described in subsections 51-30-01.2.a.(1)-(7) has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable. ~~that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.~~ Good faith acquisition of personal information for the purposes of the person maintaining the information by an employee or agent of the person is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

2. a. "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when ~~either~~ the name ~~or~~ and the data elements are not encrypted:

(1) The individual's social security number;

(2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;

(3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;

(4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code or password that would permit access to an individual's account;

(5) The individual's date of birth;

(6) The maiden name of the individual's mother; or

~~(7) An identification number assigned to the individual by the individual's Employer~~ The individual's digitized or other electronic signature.

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

**51-30-02. Notice to consumers.** Any person that conducts business in North Dakota, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in section 51-30-04, or any measures necessary to determine the scope of the breach and to restore the integrity of the data system.

**51-30-03. Notice to owner or licensee of personal information.** Any person that maintains computerized data that includes personal information that the person does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following the discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

**51-30-04. Delayed notice.** The notification required by this chapter may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this chapter must be made after the law enforcement agency determines that the notification will not compromise the investigation.

**51-30-05. Method of notice.** Notice under this chapter may be provided by one of the following methods:

1. Written notice;

2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of Title 15 of the United States Code; or

3. Substitute notice, if the person demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or the person does not have sufficient contact information. Substitute notice ~~includes~~ shall consist of all of the following:

a. E-mail notice when the person has an email address for the subject persons;



b. Conspicuous posting of the notice on the person's web site page, if the person maintains one; or and

c. Notification to major statewide media.

**51-30-06. Alternate compliance.** Notwithstanding section 51-30-05, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of ~~section 51-30-05~~, this chapter is deemed to be in compliance with the notification requirements of this chapter if the person notifies subject individuals in accordance with its policies in the event of a breach of security of the system. A financial institution, trust company or credit union that is subject to, examined for, and in compliance with the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with the requirements of this chapter.

**51-30-07. Enforcement - Powers - Remedies - Penalties.** The attorney general may enforce this chapter. The attorney general, in enforcing this chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter 51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties, prohibitions, and penalties of this chapter are not exclusive and are in addition to all other causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.

**SECTION 4. EMERGENCY.** This Act is declared to be an emergency measure.