

# MICROFILM DIVIDER

OMB/RECORDS MANAGEMENT DIVISION

SFN 2053 (2/85) 5M



ROLL NUMBER

DESCRIPTION

2191

2001 SENATE INDUSTRY, BUSINESS AND LABOR

SB 2191

2001 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2191

Senate Industry, Business and Labor Committee

Conference Committee

Hearing Date January 23, 2001.

Tape Number	Side A	Side B	Meter #
1	x		24.2 to end
1		x	0 to 23.9
(Jan. 31/01) 3		x	36.4 to 38.9
(Feb. 12/01) 2	x		8.7 to 37.2
(April 4/01) 1	x		0 to 25.8

Committee Clerk Signature

*Doris E. Pires*

Minutes:

The meeting was called to order. All committee members present. Hearing was opened on SB 2191 relating to disclosure of financial information by financial institutions.

SENATOR KREBSBACH: presented bill.

MARILYN FOSS, ND Bankers Assn. In favor. Written testimony attached. This bill makes information sharing rules for providers of financial services inside and outside of ND the same. As law is now small banks are unable to share information with unaffiliated data processing vendor without customer's consent. This was not the intent and places small institutions in a significant competitive disadvantage.

SENATOR ESPEGARD: Bank wouldn't be able to sell information to third parties?

M FOSS: Subject to GLB provisions on information sharing practices, disclosing account information to third parties for marketing purposes is prohibited.

Page 2  
Senate Industry, Business and Labor Committee  
Bill/Resolution Number SB 2191  
Hearing Date January 23, 2001.

SENATOR D. MATHERN: My concern is that the way it is written would require people to "opt in".

M FOSS: This bill adopts GLB philosophy, give customers choice, institution notifies them, they are required to act.

SENATOR TOLLEFSON: If I choose no, I would have to contact bank to stop information sharing.

M FOSS: Correct.

JOEL GILBERTSON, Executive VP, Independent Community Banks of ND. In favor of this bill. Written testimony attached.

GARY PRESZLER, Commissioner, Dept. of Banking and Financial Institutions. Neutral, to inform. Written testimony attached.

January 31/01. Tape 3-B-36.4 to 38.9

Committee reconvened. All members present. Discussion held. Action held pending amendments to be submitted by MARILYN FOSS, to fill gaps and eliminate ambiguity.

Feb. 12/01 Tape 2-A- 8.7 to 37.2

Committee reconvened. All members present.

MARILYN FOSS, NDBA. Written testimony submitted explaining amendments and definitions.

Discussion held. SENATOR ESPEGARD: Motion to adopt amendments. SENATOR

TOLLEFSON: Second. Roll call vote: 7 yes; 0 no. Motion carried.

SENATOR ESPEGARD: Motion: do pass as amended. SENATOR D. MATHERN: Seconded.

Roll call vote: 7 yes; 0 no. Carrier: SENATOR KREBSBACH.

Page 3

Senate Industry, Business and Labor Committee

Bill/Resolution Number SB 2191

Hearing Date January 23, 2001.

April 3/01. Tape 1-A-0 to 25.8

Committee reconvened. All members present.

**Marilyn Foss**, NDBA, House amended bill by adding sections 3 and 5. Section 3 extends opt out rights and disclosure requirements that consumers have both under federal and state laws to agricultural and commercial accounts. GLB only covers consumers, including agricultural and commercial was supported by the financial institutions. Section 3 incorporates service provider and other exceptions of GLB into agriculture and commercial section to make clear that bank or credit union can use customer information for third party service provider agreements. Without that part of section 3 smaller banks and credit unions would be subject to charges that they are violating ND banking law when using third party service providers. Sunset on section 3 coincides with SCR 4019 which is the study of privacy.

**Senator Mutch:** What kind of information can be passed out?

**M Foss:** Only the information necessary to do the processing.

**Senator Tollefson:** Only the amendment sunsets after two years? What if the entire bill would not be brought into law until after the study resolution is completed?

**M Foss:** ND would be out of step with the now national system of customer information protection and sharing. It would place all institutions at risk of being charged with violating ND laws and would also place ND banks and credit unions at a competitive disadvantage.

Committee discussed misinformation on the press regarding this bill and stressed it will be up to the customer whether information is sold or not.

**Senator Mathern:** The people who handle the information are considered agents and therefore exempt from the law?

**M Foss:** Usually contract specify they cannot sell information. Many also specify they are not

**O**

**O**

**N**

**T**

**NEXT FICHE**

Page 4

Senate Industry, Business and Labor Committee

Bill/Resolution Number SB 2191

Hearing Date January 23, 2001.

agents because the financial institutions don't want to transfer liability. Our present law doesn't provide exception for service providers.

**Greg Tschider**, ND Credit Union League. We are presently in violation of law by exchanging information. We will have to reevaluate how we provide services to customers. Right now if you don't want the information on your drivers' license sold you have to opt out. All we are asking is lets use the same system for financial institutions. We need this bill and would appreciate your support.

Discussion held.

**Senator Espgaard:** GLB says you have to notify your customers by July 1st of this year. GLB is to put all in a leveled playing field.

**Senator Klein:** Motion to concur with House amendments. **Senator Espgaard:** Second.

Roll call vote: 7 yes; 0 no. Motion carried. Floor assignment: **Senator Krebsbach.**

18273.0101  
Title.

Prepared by the Legislative Council staff for  
Senators Krebsbach, Espegard  
January 29, 2001

PROPOSED AMENDMENTS TO SENATE BILL NO. 2191

Page 1, line 2, after "institutions" insert "; to provide an effective date; and to declare an emergency"

Page 1, after line 9, insert:

**"SECTION 2. EFFECTIVE DATE.** Section 1 of this Act becomes effective on July 1, 2001.

**SECTION 3. EMERGENCY.** This Act is declared to be an emergency measure."

Renumber accordingly







REPORT OF STANDING COMMITTEE

SB 2191: Industry, Business and Labor Committee (Sen. Mutch, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (7 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2191 was placed on the Sixth order on the calendar.

Page 1, line 2, after "institutions" insert "; to amend and reenact section 6-08.1-01 of the North Dakota Century Code, relating to the definition of a customer and customer information; to provide an effective date; and to declare an emergency"

Page 1, after line 3, insert:

**"SECTION 1. AMENDMENT.** Section 6-08.1-01 of the 1999 Supplement to the North Dakota Century Code is amended and reenacted as follows:

**6-08.1-01. Definitions.** As used in this chapter:

1. "Customer" means, with respect to a financial institution, any ~~person who has transacted or is transacting business with, or has used or is using the services of~~ individual or authorized representative of an individual to whom a financial institution, ~~or for whom a financial institution has acted~~ provides a product or service for personal, family, or household use, including that of acting as a fiduciary ~~with respect to trust property.~~
2. "Customer information" means ~~either of the following:~~
  - a. ~~Any original or any copy of any records held by a financial institution pertaining to a customer's relationship with the financial institution.~~
  - b. ~~Any information derived from a record described in this subsection~~ nonpublic personal information maintained by or for a financial institution which is derived from a customer relationship between the financial institution and a customer of the financial institution and is identified with the customer.
3. "Financial institution" means any organization authorized to do business under state or federal laws relating to financial institutions, including, without limitation, a bank, including the Bank of North Dakota, a savings bank, a trust company, a savings and loan association, or a credit union.
4. "Financial institution regulatory agency" means any of the following:
  - a. The federal deposit insurance corporation.
  - b. The federal savings and loan insurance corporation.
  - c. The national credit union administration.
  - d. The federal reserve board.
  - e. The United States comptroller of the currency.
  - f. The department of banking and financial institutions.
  - g. The federal home loan bank board.

5. "Governmental agency" means any agency or department of this state, or any authorized officer, employee, or agent of an agency or department of this state.
6. "Law enforcement agency" means any agency or department of this state or of any political subdivision of this state authorized by law to enforce the law and to conduct or engage in investigations or prosecutions for violations of law.
7. "Person" means any individual, partnership, corporation, limited liability company, association, trust, or other legal entity."

Page 1, underscore lines 6 through 9

Page 1, after line 9, insert:

**"SECTION 3. EFFECTIVE DATE.** This Act becomes effective on July 1, 2001.

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

Renumber accordingly

Date: April 3/01  
Roll Call Vote #: 1

2001 SENATE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. 2191

Senate Industry, Business and Labor Committee

- Subcommittee on \_\_\_\_\_  
or  
 Conference Committee

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

Action Taken Do concur with House amendments

Motion Made By Sen Klein Seconded By Sen Espgaard

Senators	Yes	No	Senators	Yes	No
Senator Mutch - Chairman	✓		Senator Every	✓	
Senator Klein - Vice Chairman	✓		Senator Mathern	✓	
Senator Espgaard	✓				
Senator Krebsbach	✓				
Senator Tollefson	✓				

Total (Yes) 7 No 0

Absent 0

Floor Assignment Sen Krebsbach

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

2001 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2191

2001 HOUSE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2191

House Industry, Business and Labor Committee

Conference Committee

Hearing Date March 14, 2001

Tape Number	Side A	Side B	Meter #
1	X	X	0
			-16.9
Committee Clerk Signature <i>Deidra</i>			

Minutes: Chairman R. Berg, Vice-Chair G. Keiser, Rep. M. Ekstrom, Rep. R. Froelich, Rep. G. Froseth, Rep. R. Jensen, Rep. N. Johnson, Rep. J. Kasper, Rep. M. Klein, Rep. Koppang, Rep. D. Lemieux, Rep. B. Pietsch, Rep. D. Ruby, Rep. D. Severson, Rep. E. Thorpe.  
Sen. Karen Krebsbach: Sponsor of bill with **written testimony**.

Marilyn Foss: *NDBA* Support bill with **written testimony**.

Rep. Kasper: (19.2) What would happen without SB 2191?

Foss: The effectiveness would depend on the FTC opinion, this bill gives specific definitions.

Rep. Kasper: So an affiliate of a bank is exempt. With this, will consumers have more protection?

Foss: More than with GLB.

Rep. Jensen: How did the bill evolve?

Foss: There was inconsistent interpretations.

Tim Karsky: (31.1) *Dept. of Banking* provided neutral **written testimony**.

Page 2

House Industry, Business and Labor Committee

Bill/Resolution Number SB 2191

Hearing Date March 14, 2001

Rep. Jim Kasper: **Written testimony** opposed to bill.

Jennifer Ring: Opposed to bill. Opt-in is the law in several states and is becoming a big trend.

The consumer deserves the right to their private information. Current law is far better than

SB 2191.

Greg Tschider: *ND Credit Union League* support bill with **written testimony**.

Rep. Lemjeux: Are commercial farmers afforded protection with this?

Tschider: The law would be silent in that matter so it depends on each bank.

Rep. Ruby: (10.5) I thought that state rules would super cede federal laws. Why doesn't to of state banks apply to that?

Tschider: Existing federal law preempts state law.

Joel Gilbertson: *Ind. Com. Banks ND* support bill with **written testimony**.

Rep. Jensen: Do banks supply information to Dunn and Bradstreet?

Gilbertson: Some do and some don't.

Leah Coghlan: *American Insurance Assoc.* We support this bill.

Chairman Berg: We'll close the hearing on SB 2191.

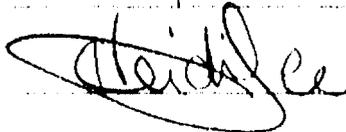
2001 HOUSE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2191(B)

House Industry, Business and Labor Committee

Conference Committee

Hearing Date March 20, 2001

Tape Number	Side A	Side B	Meter #
1	X		56.9
1		X	-34.2
Committee Clerk Signature 			

Minutes: Chairman R. Berg, Vice-Chair G. Keiser, Rep. M. Ekstrom, Rep. R. Froelich, Rep. G. Froseth, Rep. R. Jensen, Rep. N. Johnson, Rep. J. Kasper, Rep. M. Klein, Rep. Koppang, Rep. D. Lemieux, Rep. B. Pietsch, Rep. D. Ruby, Rep. D. Severson, Rep. E. Thorpe.

Rep Severson: Overview of bill and provided amendments, moved adoption of.

Rep Pietsch: Second.

Rep Kasper: Explained what section 3 of the amendment does.

Rep Severson: The bank has to provide information to their ag. and commercial customers.

Chairman Berg: GLB is silent on commercial and ag nation wide. The object is to make customers aware of banks' policies.

Rep Ruby: Is this in addition to GLB?

Chairman Berg: Yes.

Rep Ruby: So this makes the law more stringent in the state.

Chairman Berg: If this is passed it will be consistent with federal law.

Page 2

House Industry, Business and Labor Committee

Bill/Resolution Number SB 2191(B)

Hearing Date March 20, 2001

Rep Ruby: Moving these amendments will change our conformity.

Rep Kasper: This bill does nothing but add in the ag and commercial customers. This bill does nothing for protecting information from being shared.

Rep Severson: Logically any bank will allow you to opt-out.

Rep Lemieux: If every bank is selling this information then logically the bank doesn't need to offer opt-out.

Rep Ruby: If we change this to allow the opt-out we'll be superseding federal law and be under federal review.

Rep Severson: If we wait to do this it will be too late.

Rep Ruby: Too late for what? Do they have to follow ND law until we change?

Chairman Berg: Yes, if ND law is stronger.

Vice-Chairman Keiser: Currently we have opt-in. If we are ruled against in a court of law then GLB takes over.

Rep Kasper: GLB is the law throughout the US. The only issue left is the privacy issue and that power has been given to the states. ND protects our customers more in this. If we pass 2191 we will have given the power to the federal trade commission.

Rep Ruby: I'm for the amendment.

Rep Ekstrom: As far as ag, are they in agreement with this?

Rep Severson: I don't have that input.

Rep M. Klein: Why have an expiration date?

Chairman Berg: To watch GLB as it evolves and to keep updated.

Rep Lemieux: I think we are fixing something that isn't broken. This isn't worth doing anything.

Page 3

House Industry, Business and Labor Committee

Bill/Resolution Number SB 2191(B)

Hearing Date March 20, 2001

Rep Severson: I move a do pass as amended.

Rep Jensen: I second.

8 yea, 6 nay, 1 absent    Carrier Rep Severson

2001 HOUSE STANDING COMMITTEE MINUTES

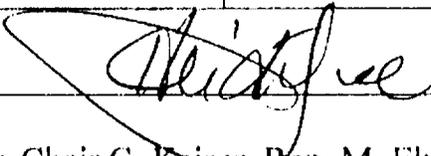
BILL/RESOLUTION NO. SB 2191(C)

House Industry, Business and Labor Committee

Conference Committee

Hearing Date March 21, 2001

Tape Number	Side A	Side B	Meter #
1	X		0-35.5

Committee Clerk Signature 

Minutes: Chairman R. Berg, Vice-Chair G. Keiser, Rep. M. Ekstrom, Rep. R. Froelich, Rep. G. Froseth, Rep. R. Jensen, Rep. N. Johnson, Rep. J. Kasper, Rep. M. Klein, Rep. Koppang, Rep. D. Lemieux, Rep. B. Pietsch, Rep. D. Ruby, Rep. D. Severson, Rep. E. Thorpe.

Rep Severson: I move to reconsider SB 2191.

Rep Ekstrom: I second.

Rep Severson: Provided and explained amendments 18273.0202.

Rep Ekstrom: I definitely like this better.

Rep Kasper: Nonpublic information is financial statements and so forth.

Rep Ruby: I'd like to toughen this up. We shouldn't muddy this up by confusing GLB with current state law.

Rep Severson: I move to reconsider the amendments.

Rep Ekstrom: I second.

Rep Severson: I move the .0202 amendments.

Page 2

House Industry, Business and Labor Committee

Bill/Resolution Number SB 2191(C)

Hearing Date March 21, 2001

Rep Ekstrom: I second.

Rep Severson: GLB will be changing and with the expiration we would have a chance to look at this again.

Rep Kasper: GLB's option is on an annual basis.

Rep Ruby: I'm going to resist the amendment.

Chairman Berg: With GLB being silent in this area, the amendment is compliant.

Vice-Chairman Keiser: There is no federal law in this area at all.

Marilyn Foss: 6-08.1 provides the exemptions.

Rep Kasper: We need to include a time frame.

Rep Jensen: I think we should add in annually.

Rep Kasper: We also need to specify opt-in or opt-out.

Vice-Chairman Keiser: I think the language says opt-out.

Chairman Berg: I see where in may be opt-in.

Rep Kasper: I think that it just needs to be consistent.

Joel Gilbertson:(22.2) The second line makes it clear for them to opt-in.

Rep Ruby: Why can banks be more stringent than GLB but the states can't?

Rep Kasper: I'd like to strike out section five.

Rep Severson: I move a do pass as amended.

Rep M. Klein: I second.

Rep Kasper: I have a new amendment being prepared.

Rep Severson: I withdraw the motion.

Rep M. Klein: I agree.

PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2191

Page 1, line 1, after "6-08.1-02" insert "and a new section to chapter 6-08.1"

Page 1, line 2, after "institutions" insert "and notification of privacy policies"

Page 1, line 4, after the second semicolon insert "to provide an expiration date;"

Page 2, after line 23, insert:

**"SECTION 3.** A new section to chapter 6-08.1 of the North Dakota Century Code is created and enacted as follows:

**Agricultural and commercial accounts.** A financial institution shall notify the financial institution's agricultural and commercial customers in this state of the financial institution's privacy policies and practices relating to agricultural and commercial accounts."

Page 2, after line 24, insert:

**"SECTION 5. EXPIRATION DATE.** Section 3 of this Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

Date: 3-20-01  
Roll Call Vote #: 1

2001 HOUSE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 2191

House Industry, Business and Labor Committee

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

Action Taken move amendment

Motion Made By Severson Seconded By Pietsch

Representatives	Yes	No	Representatives	Yes	No
Chairman- Rick Berg	✓		Rep. Jim Kasper		✓
Vice-Chairman George Keiser			Rep. Matthew M. Klein	✓	
Rep. Mary Ekstorm	✓		Rep. Myron Koppang	✓	
Rep. Rod Froelich	✓		Rep. Doug Lemieux		✓
Rep. Glen Froseth	✓		Rep. Bill Pietsch	✓	
Rep. Roxanne Jensen	✓		Rep. Dan Ruby	✓	
Rep. Nancy Johnson		✓	Rep. Dale C. Severson	✓	
			Rep. Elwood Thorpe	✓	

Total (Yes) 11 No 3

Absent 1

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

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



PROPOSED AMENDMENTS TO ENGROSSED SENATE BILL NO. 2191

Page 1, line 1, after "6-08.1-02" insert "and a new section to chapter 6-08.1"

Page 1, line 2, after "Institutions" insert "and notification of privacy policies"

Page 1, line 4, after the second semicolon insert "to provide an expiration date;"

Page 2, after line 23, insert:

**"SECTION 3.** A new section to chapter 6-08.1 of the North Dakota Century Code is created and enacted as follows:

**Agricultural and commercial accounts.**

1. A financial institution shall notify the financial institution's agricultural and commercial customers in this state of the financial institution's privacy policies and practices relating to agricultural and commercial accounts.
2. If the financial institution discloses nonpublic information about agricultural or commercial accounts to nonaffiliated third parties, the financial institution shall allow agricultural and commercial customers to not agree to disclosing that information. An agricultural or commercial customer also may agree to the disclosure of nonpublic information.
3. The exceptions in section 502(b)(2) of the Gramm Leach Bliley Financial Service Modernization Act [Pub. L. 106-102; 113 Stat. 1437; 15 U.S.C. 6802] and section 6-08.1-02 apply to agricultural and commercial accounts."

Page 2, after line 24, insert:

**"SECTION 5. EXPIRATION DATE.** Section 3 of this Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

Date: 3-21-01  
Roll Call Vote #: 2

2001 HOUSE STANDING COMMITTEE ROLL CALL VOTES  
BILL/RESOLUTION NO. SB 2191

House Industry, Business and Labor Committee

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

Action Taken amend. 202

Motion Made By Severson Seconded By Ekstorm

Representatives	Yes	No	Representatives	Yes	No
Chairman- Rick Berg	✓		Rep. Jim Kasper	✓	
Vice-Chairman George Keiser	✓		Rep. Matthew M. Klein	✓	
Rep. Mary Ekstorm	✓		Rep. Myron Koppang	✓	
Rep. Rod Froelich	✓		Rep. Doug Lemieux	✓	
Rep. Glen Froseth	✓		Rep. Bill Pietsch	✓	
Rep. Roxanne Jensen	✓		Rep. Dan Ruby		✓
Rep. Nancy Johnson	✓		Rep. Dale C. Severson	✓	
			Rep. Elwood Thorpe	✓	

Total (Yes) 14 No 1

Absent 0

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

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

**REPORT OF STANDING COMMITTEE**

SB 2191, as engrossed: Industry, Business and Labor Committee (Rep. Berg, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (8 YEAS, 6 NAYS, 1 ABSENT AND NOT VOTING). Engrossed SB 2191 was placed on the Sixth order on the calendar.

Page 1, line 1, after "6-08.1-02" insert "and a new section to chapter 6-08.1"

Page 1, line 2, after "institutions" insert "and notification of privacy policies"

Page 1, line 4, after the second semicolon insert "to provide an expiration date;"

Page 2, after line 23, insert:

**"SECTION 3.** A new section to chapter 6-08.1 of the North Dakota Century Code is created and enacted as follows:

Agricultural and commercial accounts. A financial institution shall notify the financial institution's agricultural and commercial customers in this state of the financial institution's privacy policies and practices relating to agricultural and commercial accounts."

Page 2, after line 24, insert:

**"SECTION 5. EXPIRATION DATE.** Section 3 of this Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

VR  
3/27/01  
1082

**HOUSE AMENDMENTS TO ENGROSSED SENATE BILL 2191 IRL 03-28-01**  
Page 1, line 1, after "enact" insert "two new subsections to section 6-08.1-01," and after  
"6-08.1-02" insert ", a new section to chapter 10-04, and a new section to chapter  
26.1-02"

Page 1, line 2, after "Code" insert "and to create and enact a new section to Senate Bill  
No. 2127, as approved by the fifty-seventh legislative assembly" and after "institutions"  
insert "and the effective date of section 1 of Senate Bill No. 2127"

Page 1, line 4, replace "definition of a customer and" with "definitions relating to disclosure of"  
and after "date" insert "; to provide an expiration date"

Page 1, line 10, remove ", with respect to a financial institution," and remove the overstrike over  
"~~person who has~~"

Page 1, remove the overstrike over line 11

Page 1, line 12, remove "individual or authorized representative of an individual to whom"

Page 1, line 13, remove the overstrike over ", or for whom a financial institution has acted" and  
remove "provides a product or"

Page 1, line 14, remove "service for personal, family, or household use, including that of acting"

Page 1, line 15, remove the overstrike over "with respect to trust property"

Page 1, line 19, after "~~subsection~~" insert "any" and after "~~nonpublic~~" insert ", personally  
identifiable financial information of a customer which is obtained by the financial  
institution by any means, except for information that is otherwise publicly available"

Page 1, remove lines 20 and 21

Page 1, line 22, remove "customer of the financial institution and is identified with the customer"

**HOUSE AMENDMENTS TO ENGROSSED SENATE BILL 2191 IRL 03-28-01**  
Page 2, line 3, overstrike "means any of the following" and insert immediately thereafter  
"includes"

Page 2, overstrike lines 16 and 17

Page 2, after line 17, insert:

**"SECTION 2.** Two new subsections to section 6-08.1-01 of the 1999  
Supplement to the North Dakota Century Code are created and enacted as follows:

"Affiliate" means any company that controls, is controlled by, or is under  
common control with another company.

"Nonaffiliated third party" means any entity that is not an affiliate of, or  
related by common ownership or affiliated by corporate control with, the  
financial institution. The term does not include a joint employee of such a  
financial institution."

2082

**"SECTION 4.** A new section to chapter 10-04 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every dealer, agent, investment adviser, federal covered adviser, and investment adviser representative is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section.

**SECTION 5.** A new section to chapter 26.1-02 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every insurance company, nonprofit health service corporation, and health maintenance organization is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section.

**SECTION 6.** A new section to Senate Bill No. 2127, as approved by the fifty-seventh legislative assembly, is created and enacted as follows:

**SECTION 3. EFFECTIVE DATE.** Section 1 of this Act becomes effective on August 1, 2003."

Page 2, line 24, after "DATE" insert "- EXPIRATION DATE", replace "This" with "Sections 1, 4, 5, 6, 7, and 8 of this", replace "becomes" with "become", after "2001" insert ", and sections 2 and 3 of this Act become effective on August 1, 2003", and after the period insert "Sections 4 and 5 of this Act are effective through July 31, 2003, and after that date are ineffective."

Re-number accordingly



REPORT OF STANDING COMMITTEE (MINORITY)

SB 2191, as engrossed: Industry, Business and Labor Committee (Rep. Berg, Chairman) A MINORITY of your committee (Reps. Keiser, Kasper, Lemieux, Ruby) recommends AMENDMENTS AS FOLLOWS and when so amended, recommends DO PASS.

Page 1, line 1, after "enact" insert "two new subsections to section 6-08.1-01," and after "6-08.1-02" insert ", a new section to chapter 10-04, and a new section to chapter 26.1-02"

Page 1, line 2, after "Code" insert "and to create and enact a new section to Senate Bill No. 2127, as approved by the fifty-seventh legislative assembly" and after "institutions" insert "and the effective date of section 1 of Senate Bill No. 2127"

Page 1, line 4, replace "definition of a customer and" with "definitions relating to disclosure of" and after "date" insert "; to provide an expiration date"

Page 1, line 10, remove ", with respect to a financial institution," and remove the overstrike over "person who has"

Page 1, remove the overstrike over line 11

Page 1, line 12, remove "individual or authorized representative of an individual to whom"

Page 1, line 13, remove the overstrike over ", or for whom a financial institution has acted" and remove "provides a product or"

Page 1, line 14, remove "service for personal, family, or household use, including that of acting"

Page 1, line 15, remove the overstrike over "~~with respect to trust property~~"

Page 1, line 19, after "~~subsection~~" insert "any" and after "~~nonpublic~~" insert ", personally identifiable financial information of a customer which is obtained by the financial institution by any means, except for information that is otherwise publicly available"

Page 1, remove lines 20 and 21

Page 1, line 22, remove "customer of the financial institution and is identified with the customer"

Page 2, line 3, overstrike "means any of the following" and insert immediately thereafter "includes"

Page 2, overstrike lines 16 and 17

Page 2, after line 17, insert:

**"SECTION 2.** Two new subsections to section 6-08.1-01 of the 1999 Supplement to the North Dakota Century Code are created and enacted as follows:

"Affiliate" means any company that controls, is controlled by, or is under common control with another company.

"Nonaffiliated third party" means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the

financial institution. The term does not include a joint employee of such a financial institution."

Page 2, after line 23, insert:

**"SECTION 4.** A new section to chapter 10-04 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every dealer, agent, investment adviser, federal covered adviser, and investment adviser representative is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section.

**SECTION 5.** A new section to chapter 26.1-02 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every insurance company, nonprofit health service corporation, and health maintenance organization is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section.

**SECTION 6.** A new section to Senate Bill No. 2127, as approved by the fifty-seventh legislative assembly, is created and enacted as follows:

**SECTION 3. EFFECTIVE DATE.** Section 1 of this Act becomes effective on August 1, 2003."

Page 2, line 24, after "DATE" insert "- EXPIRATION DATE", replace "This" with "Sections 1, 4, 5, 6, 7, and 8 of this", replace "becomes" with "become", after "2001" insert ", and sections 2 and 3 of this Act become effective on August 1, 2003", and after the period insert "Sections 4 and 5 of this Act are effective through July 31, 2003, and after that date are ineffective."

Renumber accordingly

The reports of the majority and the minority were placed on the Seventh order of business on the calendar for the succeeding legislative day.

VR  
3/27/01  
SD

**HOUSE AMENDMENTS TO ENGROSSED SENATE BILL 2191 IBL 03-28-01**  
Page 1, line 1, after "6-08.1-02" insert "and a new section to chapter 6-08.1"

Page 1, line 2, after "institutions" insert "and notification of privacy policies"

Page 1, line 4, after the second semicolon insert "to provide an expiration date;"

**HOUSE AMENDMENTS TO ENGROSSED SENATE BILL 2191 IBL 03-28-01**  
Page 2, after line 23, insert:

"**SECTION 3.** A new section to chapter 6-08.1 of the North Dakota Century Code is created and enacted as follows:

**Agricultural and commercial accounts.**

1. A financial institution shall notify the financial institution's agricultural and commercial customers in this state of the financial institution's privacy policies and practices relating to agricultural and commercial accounts.
2. If the financial institution discloses nonpublic information about agricultural or commercial accounts to nonaffiliated third parties, the financial institution shall annually allow agricultural and commercial customers to not agree to disclosing that information. An agricultural or commercial customer also may agree to the disclosure of nonpublic information.
3. The exceptions in section 502(b)(2) of the Gramm Leach Bliley Financial Service Modernization Act [Pub. L. 106-102; 113 Stat. 1437; 15 U.S.C. 6802] and section 6-08.1-02 apply to agricultural and commercial accounts."

Page 2, after line 24, insert:

"**SECTION 5. EXPIRATION DATE.** Section 3 of this Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

**REPORT OF STANDING COMMITTEE (MAJORITY)**

**SB 2191, as engrossed: Industry, Business and Labor Committee (Rep. Berg, Chairman) A MAJORITY of your committee (Reps. Berg, Ekstrom, Froelich, Froseth, Jensen, N. Johnson, M. Klein, Koppang, Pletsch, Thorpe) recommends AMENDMENTS AS FOLLOWS and when so amended, recommends DO PASS.**

Page 1, line 1, after "6-08.1-02" insert "and a new section to chapter 6-08.1"

Page 1, line 2, after "institutions" insert "and notification of privacy policies"

Page 1, line 4, after the second semicolon insert "to provide an expiration date;"

Page 2, after line 23, insert:

**"SECTION 3.** A new section to chapter 6-08.1 of the North Dakota Century Code is created and enacted as follows:

Agricultural and commercial accounts.

1. A financial institution shall notify the financial institution's agricultural and commercial customers in this state of the financial institution's privacy policies and practices relating to agricultural and commercial accounts.
2. If the financial institution discloses nonpublic information about agricultural or commercial accounts to nonaffiliated third parties, the financial institution shall annually allow agricultural and commercial customers to not agree to disclosing that information. An agricultural or commercial customer also may agree to the disclosure of nonpublic information.
3. The exceptions in section 502(b)(2) of the Gramm Leach Bliley Financial Service Modernization Act [Pub. L. 106-102; 113 Stat. 1437; 15 U.S.C. 6802] and section 6-08.1-02 apply to agricultural and commercial accounts."

Page 2, after line 24, insert:

**"SECTION 5. EXPIRATION DATE.** Section 3 of this Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

The reports of the majority and the minority were placed on the Seventh order of business on the calendar for the succeeding legislative day.

2001 TESTIMONY

SB 2191

TESTIMONY OF MARILYN FOSS  
IN FAVOR OF SB 2191  
(On Behalf of the North Dakota Bankers Association)

Chairman Mutch, members of the Senate Industry Business and Labor Committee, my name is Marilyn Foss. I am general counsel for the North Dakota Bankers Association and am appearing here on its behalf and in favor of SB 2191. This bill amends NDCC 6-08.1-02, the statute which sets out exemptions to North Dakota's generalized prohibition against disclosures of customer information by financial institutions without the customer's prior written consent. Under SB 2191, if a financial institution disclosure of customer information is covered by federal law and complies with federal law, that disclosure is exempt from the separate provisions of NDCC Chapter 6-08.1.

The bill which became NDCC Chapter 6-08.1 was introduced in this legislative assembly at the request of the North Dakota Bankers Association in 1985. Then, as now, NDBA member banks regarded customer trust and information as things to be valued and protected. The goal in 1985 was to set out procedures for financial institutions to follow when they were confronted with demands for customer information from government agencies and other third parties. But this state law has always included a variety of exemptions so North Dakota financial institutions can conduct their ordinary business operations without specialized customer consents. And, those exemption sections have been amended several times to respond to changes in the banking industry. For example, in 1997, an exemption was added to complement in state law, the federal exemption for information sharing between a bank and its affiliates. Changes in the banking industry continue

and we believe those changes warrant another amendment to the customer information law at this time.

For one thing, laws have changed substantially since 1985. Banks operate interstate, intrastate, and throughout cyberspace. Furthermore, barriers to insulate and separate the banking, insurance and securities industries are largely gone. Every single day North Dakota banks compete with each other and with larger and smaller financial service providers from every other state. In late 1999 Congress passed a financial modernization law, the Gramm-Leach-Bliley Act ("GLB"). GLB recognized the banking industry, insurance industry and securities industry are related and competing segments of a whole financial services industry. The law repealed depression era laws which had kept the industry segmented to permitted affiliations (common ownership) among them. As a federal law GLB applies to all segments of the financial services industry and to every single North Dakota bank. One of the new GLB provisions regulates customer information sharing practices of the financial services industry. The privacy provisions have been implemented by federal banking and securities regulators and by state insurance regulators working through state legislatures and NAIC. (For example, the insurance department has sponsored a bill to require North Dakota insurers to comply with the provisions of GLB and to authorize the state insurance department to promulgate implementing regulations.) In 1985, there was no federal law. Now, there are extensive, new federal regulations that cover each financial institution's customer information sharing practices and policies and requirements for secure systems to protect against unauthorized access to customer information by third parties. As a result North Dakota banks ( and those in every other state)

have been analyzing the circumstances under which customer information is shared with nonaffiliated third parties and have been developing policies in order to give every customer written notice of the practices and policies by July 1, 2001, and at least annually after that. Under the federal regulations, financial institutions will also notify customers that they have a choice and can direct the financial institution not to disclose covered information to nonaffiliated third parties and will tell customers how to exercise that choice.

With GLB, North Dakota bankers now face two major dilemmas.

The first is to figure out how to comply with both sets of law when they are similar, but not the same, in many areas, and inconsistent in other areas. GLB preempts "inconsistent" state laws on the subject of financial institution customer information disclosures unless the Federal Trade Commission concludes an inconsistent state law is "stronger" than GLB. I think it is fair to say that most people believe current North Dakota law is inconsistent with GLB provisions for notice, "opt out" and permissible information sharing with nonaffiliated third parties, for example. What's not so clear is whether the FTC will regard the law as being stronger or not, and, if not, whether the preemption will be partial or total.

The second is how to effectively compete with financial service providers which are not subject to North Dakota's customer information law.

Even the smallest North Dakota bank now operates in actual, day by day competition with financial institutions and financial service providers throughout the United States. **Yet, Ch. 6-08.1 only applies to North Dakota**

**financial institutions. It doesn't apply to North Dakota insurance companies or securities firms , or to any financial institution or financial service provider outside the state.** If the rules which apply to our banks are different than those which apply to their in-state and out of state competitors, North Dakota banks are harmed and their ability to provide service to their customers is harmed. The harm is tangible .

Even if GLB hadn't become law, Ch. 6-08.1 needed to be amended because its literal terms don't accommodate the modern day operations of banks which don't have affiliates to perform specialized services for them. In short, current North Dakota law doesn't include an exemption to clearly permit financial institutions to outsource servicing, such as data and check processing or credit card processing, to nonaffiliated third party providers without the need to obtain customer consent. And, current law also isn't clear about joint marketing contracts with non-affiliated third parties. These types of outsourcing are completely common in the banking industry today, although they were not in 1985. Frankly, it was only when sensitivities about customer information disclosure became so heightened that this aspect of our law was noted. I know bankers didn't think of providing information to a third party so a transaction can be processed as "disclosing" customer information and I'm fairly certain legislators didn't consider it in that context either . . . but it is information sharing and North Dakota law doesn't clearly accommodate the practices as GLB does. I want to specifically note that this is primarily an issue for smaller banks. This type of information sharing by larger banks falls within exceptions for sharing information with affiliates.

I want to point out one final thing about the bill. If this bill passes and a financial institution does something which is not addressed by federal law

or fails to comply with federal law, then the disclosure is not exempted from Ch. 6-08.1. I can't honestly say that my speculations have led me to an example of information sharing which is not addressed by federal law. But I can say that a financial institution that chooses to ignore federal requirements or is negligent in following them will be subject to enforcement by federal banking regulators and state court civil action in North Dakota.

SB 2191 makes information sharing rules for providers of financial services inside and outside North Dakota the same. It's very simple and that is very important - just as competitive equality is important in every industry. We ask you to give the bill a "Do Pass".

***Testimony in Support of S.B. 2191***  
***Joel Gilbertson***  
***Independent Community Banks of North Dakota***

Mr. Chairman and members of the Senate Industry, Business and Labor Committee, I am Joel Gilbertson, Executive Vice President and General Counsel of the Independent Community Banks of North Dakota. ICBND is a statewide association of 95 banks located in communities of all sizes throughout our great state.

Community banks have historically been very strong guardians of their customer's privacy and have had a long-standing commitment to protect the confidentiality of customer information. They have jealously guarded the privacy of their customers all over North Dakota.

Our present law is a great example of that long-standing commitment. It is as strict as any banking law in the country in the area of customer privacy. Our community banks have followed this law carefully and relatively few changes have been proposed in recent years.

All of that changed with the recent changes in the financial services industry and the recent interest in customer privacy on a national level. The Gramm-Leach-Bliley Act of 1999 has been called the most significant change in banking since the 1930's. It has significantly reduced (some would say demolished) the historical firewalls between banking, insurance and securities. The new law sought to recognize and regulate the numerous mergers, acquisitions and consolidation in the financial services industry.

In addition to recognizing these financial services industry changes, a very important part of Gramm Leach Bliley was the first venture of the federal government into the complex and controversial area of financial services privacy. A series of requirements were set up in the new law that were to be implemented by the various federal agencies regulating the industries in the new law.

Generally, the new law requires two new items. The first is notice. Financial service companies are required to give notice to customers of

their privacy policies. The other new item relates to "opt-out," a catchword that is perhaps used more than any other in describing the privacy provisions of GLB. The catchword simply means that the bank or other financial institution may share the information discussed unless the customer tells the bank not to do so. Of course, there are many pages of regulations telling the financial services provider how to give the customer the opportunity to make his or her wishes known.

Contrast this law with North Dakota law. The general rule in North Dakota is that unless permission is specifically authorized to share the information, it cannot be shared. There are specific exceptions to this general rule, but generally "opt-in" is required.

Our community banks have had few problems adhering to our law. However, there is one large discrepancy in the law. It does not recognize the changes in the financial services industry recognized by Gramm Leach Bliley. It applies only to banks and does not apply to the insurance and securities industries. Therefore, with respect to banks, our state law conflicts with this new federal law.

This gets us to the ICBND absolute top priority in this increasingly competitive financial service era. Whatever disclosure law is adopted, our community banks strongly believe that the laws and the regulations should be the same for all participants in that arena -- whether they are banks, credit unions, insurance companies or securities firms. It is for that reason we support SB 2191.

This bill seeks to make the privacy rules the same for all participants in the financial services industry, just as Gramm Leach Bliley has done. It seeks to level the competitive playing field for the insurance, securities and banking sectors. It allows all of those sectors to rely on meeting the requirements of federal law. It assures banks that if they meet the federal regulations, they will meet all of the privacy requirements necessary.

As we sit here today, there is not an even playing field. The insurance and securities play by a different set of rules. The request to allow our community banks to compete with national and international insurance and securities firms under the same set of privacy laws is not an unreasonable

one.

We ask you approval of this bill and your recommendation to the North Dakota Senate that it be enacted into law. Thank you.

TESTIMONY FOR SENATE BILL NO. 2191

Senate Industry, Business, and Labor Committee

Testimony of Gary D. Preszler, Commissioner, Department of Banking and Financial Institutions neither in support of nor in opposition to Senate Bill No. 2191.

My appearance before this Committee is to provide information to assist the Committee in making an informed decision as to the relationship of North Dakota law with the provisions of the Gramm-Leach-Bliley Bank Modernization Act of 1999 (GLBA). My testimony is not taking a position on the issue of whether opt-in or opt-out is the appropriate public policy view.

*NORTH DAKOTA PRESENT LAW*

The North Dakota Disclosure of Customer Information law (Chapter 6-08.1) was enacted by the 1985 Legislative Assembly after a request by the North Dakota Bankers Association for its introduction. Attorney General's Opinions in 1985 and 1986 opined on questions related to real estate lending and judgment creditors. The last amendment to Chapter 6-08.1 occurred in 1997, when the Legislative Assembly provided that a financial institution did not need affirmative consent to disclose customer information to an entity that is controlled or owned under common control with the financial institution (affiliates). See Section

6-08.1-02(11). Proponents of the 1997 amendments included Norwest Bank, First Bank System, and the North Dakota Bankers Association.

The North Dakota Disclosure of Customer Information law provides that a "financial institution" has a duty of confidentiality and cannot disclose any customer information to any person, governmental agency, or law enforcement agency unless affirmative consent is granted (opt-in) by the customer, or unless information is obtained through a valid legal process or specifically carved out under one of the exemptions.

It is my understanding that very few other state legislatures have ever addressed the customer privacy issue by enacting any legislation, and only the States of Alaska and Vermont have opt-in requirements.

#### *GRAMM-LEACH-BLILEY ACT*

The GLBA governs financial institutions' disclosure of non-public personal information to a non-affiliated third party. GLBA exceptions include providing non-public personal information to a non-affiliated third party to perform services for functions on behalf of the financial institutions including marketing of the financial institution's own products or services. The federal banking agencies, National Credit Union Administration, the Secretary of the Treasury, Securities and Exchange Commission, and the Federal Trade Commission were required to prescribe appropriate rules to carry out the Act. The GLBA provided that a

financial institution may not otherwise disclose non-public personal information to a non-affiliated third party unless the financial institution has first provided the consumer with an opportunity to opt-out of the release of the information.

Financial institutions must develop and disclose their privacy policies. Information that must be included in those policies is covered under GLBA and the agency rules.

Section 507(a) of the GLBA provides that a state's financial privacy law is preempted and then only to the extent that the states law or rules are "inconsistent" with the GLBA. Section 507(b) provides that a state law is "not inconsistent" and thus not preempted if it provides "protection ... greater than GLBA's privacy provisions under the Act as determined by the Federal Trade Commission after consultation with the federal functional regulator or 'other authority'". The Federal Trade Commission can make a determination on a state law on its own motion or upon the petition of any "interested party".

The federal agencies all issued similar rules that are effective November 13, 2000 on a voluntary compliance basis but mandated after July 1, 2001. The rules establish the manner and method for the initial privacy policy notice, annual notice to customers thereafter, information to be included in the privacy notice, and form and content of an opt-out notice.

*FEDERAL TRADE COMMISSION PETITION*

On September 12, 2000, I petitioned the Federal Trade Commission for a determination under the GLBA as to whether North Dakota's disclosure of customer information statute affords any person greater protection than is provided under GLBA. See attached September 12, 2000, petition. The petition was requested for several reasons. First, the Independent Community Banks of North Dakota and the North Dakota Credit Union League had informed me that they preferred the present state law. Without a determination by the FTC, on July 1, 2001, state law would have been preempted. Secondly, North Dakota financial institutions need to know the rules of the road. Without a determination, financial institutions that developed privacy policies providing for opt-out opportunities would later have to change all policies and forms if an interested party made a petition request. This burden would have been at a cost to the financial institutions. An interested party may be a financial institution itself or even a customer of that financial institution.

My petition asks the FTC for a determination that North Dakota law is not inconsistent with the federal law in two areas. First, whether North Dakota's affirmative consent (opt-in) requirement affords greater customer protection than opt-out. Second North Dakota law provides for a civil penalty for violations of Chapter 6-08.1, unlike GLBA that does not provide for any penalty.

Subsequent to my request the FTC General Counsel requested several interpretations on North Dakota law, which was responded to by the Attorney General's Office on behalf of the Department. In November, I provided additional written observations and information with the primary purpose to assert that state bank regulators are the "other authority" that should be consulted with by the FTC.

The FTC is presently waiting for responses from the federal regulatory agencies and other interested parties before the Commission acts on the petition.

I have discussed the petition on a number of occasions with a FTC attorney. Based on these discussions, it is anticipated that the FTC will determine North Dakota's affirmative consent and civil penalties afford greater protection and thus is not inconsistent with the Act. Such a determination will mean that all North Dakota financial institutions will be required to comply with GLBA provisions including the federal regulatory agencies' implementing rules except that the institution will be required to provide the customer with opt-in instead of an opt-out opportunity. The same exemptions under GLBA will also apply to North Dakota financial institutions. Therefore, North Dakota financial institutions will be required to adopt a privacy policy, must meet the initial and annual disclosure of the policies, and must provide a form for the consent by the customer or consumer. Under the GLBA all financial institutions must provide for a notice, and must provide an abbreviated opt-out form, regardless whether the financial institution

intends to disclose any non-public information to an unaffiliated third party. However, for most, if not all, North Dakota financial institutions, affirmative consent would not have to be obtained from the consumer unless the financial institution intends to sell or disclose information to the non-affiliated third party.

*SENATE BILL NO. 2191*

The effect of Senate Bill No. 2191 is to eliminate North Dakota's affirmative consent (opt-in) by defaulting to the federal opt-out provisions. Again, state law is preempted by the GLBA if it is inconsistent with the provisions of GLBA.

*REGULATORY POSITION*

Although my testimony is given neutral as to the position of opt-in or opt-out, let me make it clear that my position as a regulator for state banks and credit unions is to discourage financial institutions from releasing or selling customer information to a third party. To do so creates a potential liability against the bank and consequently is a safety and soundness concern. This is a similar position taken by the Comptroller of the Currency, the regulator for national banks. In a recent class action lawsuit, a proposed settlement against US Bancorp North Dakota bank affiliates point out the validity of this position. See *Junkert v. First Bank National Association, et al*, Cass County District Court Case No. 98-1577. US Bank agreed to a proposed class action settlement after a customer alleged the bank, without her consent, violated Chapter 6-08.1 by releasing customer

information to a telemarketer that was soliciting credit insurance for a non-affiliated underwriter. US Bank also signed a proposed settlement with a number of Attorneys General, including North Dakota Attorney General Heidi Heitkamp, as a result of an action initiated by the Minnesota Attorney General. The settlement provides that the banking organization must comply with all applicable state laws or regulations imposing stricter customer data or information disclosure requirements.

Thank you.



STATE OF NORTH DAKOTA  
DEPARTMENT OF BANKING AND FINANCIAL INSTITUTIONS

CSBS Accredited since 1993

Gary D. Preszler  
COMMISSIONER

September 12, 2000

Robert Pitofsky, Chairman  
Federal Trade Commission  
600 Pennsylvania Avenue NW  
Washington DC 20580

Dear Mr. Pitofsky:

I hereby petition the Federal Trade Commission for a determination under 15 U.S.C. 6807 as to whether North Dakota's Disclosure of Customer Information statute affords any person greater protection than is provided under the Gramm-Leach-Bliley Financial Modernization Act.

As Commissioner for the North Dakota Department of Banking and Financial Institutions my responsibilities include supervision over the business affairs of all financial institutions placed under my jurisdiction. I must also report all non-compliance with governing laws. Therefore, as the supervisor over North Dakota state-chartered banks and credit unions, I have an interest in seeking the FTC determination as to whether state law is preempted.

I have attached a copy of North Dakota Century Code Chapter 6-08.1, Disclosure of Customer Information, which was effective in 1985. I direct your attention to several subsections of North Dakota law that are in contrast to the Modernization Act:

- (1) Section 6-08.1-03(1) provides that a financial institution may not disclose customer information unless "consent is granted by the customer" (opt-in). The disclosure of customer information by a financial institution to a

2000 Schafer Street, Suite G  
Bismarck, ND 58501-1204  
Telephone (701) 328-9933  
E-Mail [banking@btigate.com](mailto:banking@btigate.com)  
Fax Number (701) 328-9955  
[www.state.nd.us/bank/banking](http://www.state.nd.us/bank/banking)

Robert Pitofsky, Chairman

September 12, 2000

Page 2

subsidiary is exempt [§ 6-08.1.02(11)], except that the subsidiary cannot disclose information to another party without customer consent.

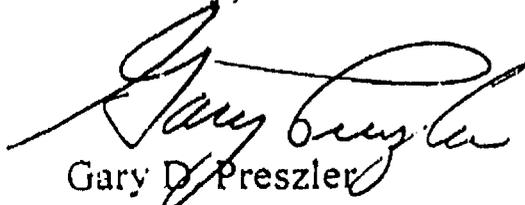
- (2) Section 6-08.1-08(1) establishes a civil penalty that may be incurred by a financial institution for violations of Chapter 6-08.1.

*Again, as an interested party, I petition the FTC for a determination as to whether North Dakota law affords greater protection to any person than is provided under the Modernization Act and, therefore, is not preempted by the Act.*

Additionally, some requirements exist under the Modernization Act that are not present in state law. For example, § 503 of the Modernization Act requires the disclosure of an institution privacy policy. Therefore, I am also asking you to address whether North Dakota state-chartered financial institutions must comply with the Modernization Act provisions not covered under North Dakota law and also with provisions of state law that are determined to afford any person greater protection.

Although Subtitle A of the Modernization Act is not effective until six months after federal banking agencies rules are presented, I ask for a determination at this time in case legislative amendments to state law become necessary.

Sincerely,



Gary D. Preszler  
Commissioner

GDP:sr  
Attachment

TESTIMONY OF MARILYN FOSS  
PROPOSED AMENDMENTS TO SB 2191

Mr. Chairman, members of the committee, my name is Marilyn Foss. I am general counsel for the North Dakota Bankers Association ( NDBA). I would like to explain the proposed amendments to SB 2191.

The purpose of SB 2191 is to conform North Dakota's requirements for disclosures of customer information to federal law after the Gramm-Leach-Bliley Financial Modernization Act of 1999 ("GLB). We want North Dakota financial institutions to be subject to the same information disclosure standards and rules as apply under state and federal law to other financial service providers inside and outside North Dakota. This committee and the Senate have accepted that premise as it applies to insurance companies and information in their possession by passing SB 2127. We are asking for the same consideration for traditional financial institutions: banks and credit unions.

But the matter is complicated by the existence of N.D.C.C. Chapter 6-08.1, a state law which applies only to banks and credit unions. We originally conceived SB 2191 as a straightforward exception to Chapter 6-08.1 under which disclosures which were covered by GLB and conformed to GLB would be excepted from the Chapter. However, during the process of the committee's consideration of SB 2191 we discovered a possible glitch with the interpretation of the exception. The banking commissioner let us know he was concerned that GLB would be interpreted as covering only consumers, while Chapter 6-08.1 presently covers commercial accounts as well. Thus, if SB 2191 passed without the amendments,

we could have an anomalous and unintended result. Banks could share consumer account information within the parameters of GLB, but, for example, couldn't share commercial account information even with third party service providers, without first obtaining the written consent of a commercial customer.

We considered how to address this and concluded the best way to do so is to narrow the scope of Chapter 6-08.1 to consumers and consumer accounts. This accords with GLB and would achieve the result originally intended by SB 2191. . . parity between North Dakota banks and financial service providers within the state and operating from outside its boundaries. We have discussed the issue with the banking commissioner and believe we agree on the interpretation that is to be given to SB 2191, with the amendments.

I want to be clear about one more thing. The bill as amended makes North Dakota an "opt-out" state. Under GLB a consumer will be given multiple notices of the right to opt out and instructions about how to exercise that right. The first notices will go out for July 1, 2001, the proposed effective date for this bill. The notices to consumers will be repeated at least once a year after that. This does give consumers a choice.

I want to point out one final thing about the approach we have taken. With these amendments, North Dakota law will clearly be a "stronger" law than GLB. . One of the major complaints about GLB is that there is no private right of action to enforce its provisions and prohibitions as they relate to disclosures of nonpublic personal financial information. Very intentionally, we have done nothing to affect the law's current provisions for a private right of action by a consumer against a

financial institution under 6-08.1-08 if there is a GLB disclosure violation.

SB 2191 as amended keeps North Dakota in the mainstream and gives our consumers stronger protections than are found in federal law. For those reasons we ask for your support of the amendments and the bill as amended.

**6-08.1-01. Definitions. As used in this chapter:**

1. "Customer means with respect to a financial institution any individual (or authorized representative of an individual) to whom a financial institution provides a product or service for personal, family, or household use, including that of acting as a fiduciary.

2. "Customer information" means any nonpublic personal information maintained by or for a financial institution which is derived from a customer relationship between the financial institution and a customer of the financial institution and is identified with the customer.

## PROPOSED AMENDMENTS TO SB 2191

Page 1, line 2, after "institutions" insert ", to amend and reenact subsection 1 and subsection 2 of section 6-08.1-02 of the 1999 Supplement to the North Dakota Century Code, relating to the definition of a customer and customer information, and to establish an effective date.

Page 1, after line 9, insert:

**SECTION 2. AMENDMENT.** Subsection 1 and subsection 2 of section 6-08.1-02 of the 1999 Supplement to the North Dakota Century Code is amended and reenacted as follows:

**6-08.1-01. Definitions.** As used in this chapter:

1. "Customer" means with respect to a financial institution any person individual (or authorized representative of an individual) who has transacted or is transacting business with or has used or is using the services of, to whom a financial institution provides a product or service for personal, family, or household use, including that of acting or for whom a financial institution has acted as a fiduciary with respect to trust property.

2. "Customer information" means nonpublic personal information maintained by or for a financial institution which is derived from a customer relationship between the financial institution and a customer of the financial institution and is identified with the customer either of the following:

a. ~~Any original or any copy of any records held by a financial institution pertaining to a customer relationship with the financial institution.~~

b. ~~Any information derived from a record described in this section~~

3. "Financial institution" means any organization authorized to do business under state or federal laws relating to financial institutions, including, without limitation, a bank, including the Bank of North Dakota, a savings bank, a trust company, a savings and loan association, or a credit union.
4. "Financial institution regulatory agency" means any of the following: a. The federal deposit insurance corporation. b. The federal savings and loan insurance corporation. c. The national credit union administration. d. The federal reserve board. e. The United States comptroller of the currency. f. The department of banking and financial institutions. g. The federal home loan bank board.
5. "Governmental agency" means any agency or department of this state, or any authorized officer, employee, or agent of an agency or department of this state.
6. "Law enforcement agency" means any agency or department of this state or of any political subdivision of this state authorized by law to enforce the law and to conduct or engage in investigations or prosecutions for violations of law.
7. "Person" means any individual, partnership, corporation, limited liability company, association, trust, or other legal entity.

SECTION 3. EFFECTIVE DATE. This Act is effective July 1, 2001.

Renumber accordingly

# NORTH DAKOTA SENATE

STATE CAPITOL  
600 EAST BOULEVARD  
BISMARCK, ND 58505-0360

Senator Karen K. Krebsbach  
District 40  
P.O. Box 1767  
Minot, ND 58702-1767

TESTIMONY - SB 2191  
HOUSE INDUSTRY BUSINESS & LABOR COMMITTEE  
REPRESENTATIVE RICK BERG, CHAIRMAN



COMMITTEES:  
Industry, Business  
and Labor  
Government and  
Veterans Affairs,  
Chairman

The purpose of SB 2191 is to make North Dakota's laws for the disclosure of financial information consistent with the new federal law, Gramm-Leach-Bliley Financial Modernization Act. This act requires that the rules for disclosure of financial information be the same for each segment of the financial services industry, that is banks, credit unions, insurance companies and security firms.

The effective date of the bill is July 1, 2001, which is consistent with the date financial services must be compliant with GLB's requirements for first notice to consumers. This notice must include the right to opt out, and the explanation of how to opt out. Consumers will again be notified at least annually with rights of opt out. In addition, if a financial institution changes its policies, that institution must give notice and opt out instructions before they can implement the changed policy.

With SB2191, North Dakota's customer information law will be completely consistent with GLB. North Dakota will be an opt out state for consumer financial information. The opt out won't apply to commercial customers just as GLB doesn't.

Marilyn Foss, general council for the North Dakota Bankers Association, will explain the bill in greater detail. Her expertise in this area will serve you well in responding to any questions that you may have.

TESTIMONY OF MARILYN FOSS  
IN FAVOR OF ENGROSSED SB 2191

Chairman Berg, members of the House IBL Committee, I am Marilyn Foss. I am general counsel for the North Dakota Bankers Association and am appearing before you in support of engrossed SB 2191.

We believe the issues which have been raised about privacy in the face of technological and operational changes are national issues and need to be resolved in a manner which is uniform for financial institutions throughout the entire US. SB 2191 generally adopts this philosophy and changes NDCC Chapter 6-08.1 so that North Dakota banks, thrifts and credit unions will be subject to the same rules for customer information as apply under the federal Gramm Leach Bliley Financial Modernization Act (GLB) to out of state banks, and insurance companies, and securities firms within North Dakota and throughout the United States.

The bill does this by making two basic changes to Chapter 6-08.1. It revises the definitions of "customer" and "customer information" to conform to GLB definitions so as to apply the chapter specifically to consumers and information about consumer accounts and consumer transactions. (In the parlance of banking, these are "retail" customers and transactions, rather than "commercial" customers and transactions.) This was done because GLB is being interpreted by federal agencies, including the four bank regulatory agencies, the Federal Trade Commission and the federal Securities and Exchange Commission, to cover only consumer customers and consumer transactions.

When this issue was raised by the Senate IBL Committee, the commissioner of banking and financial institutions and I agreed on the

answer: the privacy issue is a consumer issue. It is related to marketing consumer products to consumers.

SB 2191 also provides that an information disclosure that is covered by federal law and complies with federal law will be exempt from Chapter 6-08.1. However, if a disclosure doesn't comply with applicable federal law, then the disclosure is left subject to Chapter 6-08.1 and its consent requirements, private right of action (i.e., the ability for a consumer to sue over the violation and to seek class action status) and its provision for actual or minimum statutory damages.

Right now, you may be thinking of this bill within the contexts of the US Bank case and GLB. I want to point out two things about that. The US Bank plaintiffs are consumers, not businesses. If SB 2191 is passed and, after July 1, 2001, a financial institution engages in exactly the same conduct as is alleged in the US Bank case consumers will have exactly the same rights to go to court and seek damages against the offending bank. Furthermore, GLB, itself, outlaws sharing account numbers or access information to non affiliated third parties (other than a consumer reporting agency) for telemarketing, direct marketing or email marketing purposes. We have asked several North Dakota banks of various sizes about whether they actually sell customer information. Without exception, they have said no. However, a couple have told us that they purchase information – but not from other financial institutions.

Beyond that, however, GLB is not the only federal law on the subject and it remains to be seen whether there are more. At present there are at least 13 federal laws which address privacy of consumer customer information. That's why we didn't draft and limit SB 2191 to only GLB.

This committee has heard considerable testimony and argument about the GLB requirements. They require banks, thrifts, credit unions, insurance companies, securities firms and others to develop written policies for information collection and sharing and to then disclose those policies to their consumer customers through initial notices which must be out on or before July 1, 2001, and, at a minimum annual notices 2001. Notices will also be given in connection with new customer relationships and applications where a customer relationship isn't ultimately established. Banks and other financial institutions must develop information collection and sharing policies and give these notices even if their policy and practice is not to share information for marketing purposes at all. There is no way to get out of giving the notices. Additionally, financial institutions which do any non exempt information sharing with third party non-affiliates must notify their consumer customers of the right to "opt out" of that process, and tell them how to exercise the opt out right. Customer convenience in this process is strongly emphasized by the rules; any financial institution which makes the opt-out process too inconvenient for consumer customers risks being found to have violated the rules and subject to enforcement by state or federal regulators and, under SB 2191, through customer lawsuits.

GLB preempts inconsistent state laws and delegates the responsibility for determining inconsistency to the Federal Trade Commission. North Dakota's current law is presently undergoing this analysis by the FTC. So far as I am aware, no other state has petitioned the agency for this determination.

After it was signed in November, 1999, GLB did set off a flurry of proposals for "stronger" state laws. Numerous bills proposed to substitute

an opt-in feature for the GLB opt out. But with the specific permission for separate state laws NOT ONE STATE HAS ADOPTED A NEW OPT IN LAW.

You have heard that a few states other than North Dakota have opt in laws. The status of those existing laws is in question because they are presumptively preempted unless there is an FTC determination of consistency with GLB. No one in those states has asked for the FTC to make that determination. Now that GLB has set a national standard states like North Dakota are responding. For example, in Vermont, a bill to make that state's law consistent with the GLB opt out approach has been unanimously recommended to pass after a committee hearing. In Tennessee, legislation is pending to exempt a GLB compliant disclosure from that state's law

Numerous states are also considering GLB related bills for insurance companies. This is simply because the insurance industry does not have a federal regulator as do banks, thrifts, credit unions, securities firms and other GLB financial institutions. In order to implement GLB requirements for insurance companies and avoid federal regulation, GLB-consistent, state laws and rules are needed. North Dakota's version of the requisite insurance legislation is SB 2127. It is based on the GLB opt out standard for non public personal information. We understand that all model legislation to cover insurance companies and which is now before the states for consideration incorporate the GLB notice and opt out approach for non public personal information. And, consistent with the approach of SB 2191, the SEC has implemented GLB for securities firms, including those in North Dakota. The SEC rules also cover only consumers and consumer

information and adopt the GLB notice and opt out for non public personal information.

To date, every state which has considered the privacy issue as a result of GLB has decided to wait and see how GLB works. Why? So as not to disadvantage local financial institutions relative to out of state competitors and to relieve them of the undue confusion and regulatory burden which occurs when there are similar, but not identical, separate state and federal laws and regulations. North Dakota financial institutions should be subject to the same, national standard.

SB 2191 doesn't make things easy for banks. It leaves our banks subject to the GLB requirements for policy development, notice, and opt out. It requires banks to honor opt out requests and, it retains penalties for banks which don't follow the rules. However, it also allows our banks, thrifts and credit unions to remain competitive with their counterparts from throughout the United States and alerts North Dakota consumers to the issue, to the practices, and to their rights.

It may be that GLB isn't the last word on the subject of privacy of consumer customer information. If more remains to be done, the resolution must be a national resolution so that throughout the US, all parties in the financial services industry are operating under the same, basic rules. That is what SB 2191 seeks to achieve. The Senate IBL committee gave unanimous, bipartisan support to this bill. We are asking this committee to also give the bill a strong Do Pass recommendation.

Thank you.

## North Dakota House Industry Business and Labor Committee

Testimony of Representative Jim Kasper

SB 2191, March 14, 2001

Mr. Chairman and members of the Committee, SB 2191 has the potential to be the most egregious anti-consumer piece of Legislation that has come before this Legislative body and this Committee in years. Passage of SB 2191 will tear down the protections the people of ND have under current ND Banking law regarding their private non-public financial information by allowing ND's banks and financial institutions to share, sell and disseminate their customers financial information virtually at their will. Let me explain:

When Congress enacted the Gramm Leach Bliley Act in 1999, it tore down the barriers between the Banking, Insurance and Securities Industries that have been in effect for over 50 years, by allowing these financial service industries to own, market and distribute each others products and services. Everybody can now be in everybody else's business. There are no more barriers.

In the Gramm Leach Bliley Act, the Congress enacted financial privacy rules and guidelines. **For affiliated companies**, meaning those Banking, Insurance and Securities Companies **with common ownership**, the customers' non-public personal and financial information can be shared freely back and forth amongst these affiliated companies, **without the customers consent or knowledge**. To sell or distribute this information to outside **non-affiliated companies**, (no common ownership) the financial institutions will send a Privacy Notice to its customers once a year. If the customer does not sign a form and mail it back to the institution to **OPT OUT**, the information can be sold to outside entities.

As an example, when a customer applies for a consumer loan, such as a car or a home, the

Bank gathers the customers tax returns, financial statements and any other information it desires and makes a determination, based on the customers credit worthiness, income, debt, etc., whether or not it will make that loan to the customer. The bank gathers a great amount of customers confidential information in this process. There is nothing wrong with these practices because to protect the solvency of the bank, it must gather and inspect this kind of information to determine whether or not to make loans. But, the problem begins once you have become a customer of that bank. Under current North Dakota law, which has been in effect since 1985, the bank cannot share, sell or distribute its' customer's personal non-public financial information to **outside non-affiliated companies** or business, without first obtaining the written consent of its customer. This is called the "**OPT IN**" financial protection for North Dakota customers. Information can only be disclosed after the customer has been notified, asked if it is ok, and has provided a written consent to the Bank in advance, allowing the sharing or sale of that customers private information.

SB 2191 will change these customer protections in North Dakota banking law. If enacted, SB 2191 will supercede current North Dakota banking law, regarding our **OPT IN** protection of non-public financial information, by imposing the privacy rules of Gramm Leach Bliley on North Dakota's bank customers. Gramm Leach Bliley's approach to how banks can share private, non-public customer financial information with **non-affiliated** companies is **OPT OUT**. (**Non-affiliated** companies are those entities that have no common ownership.) An example is what happened last year in Minnesota when US Bank sold it's customers' private financial information to a telemarketing company it had no ownership in. That telemarketing company used the bank's customers financial information and sold these bank customers millions of dollars of merchandise. US Bank received a kick-back from the telemarketing company for providing the customer information.

Attorney General Hatch brought action against US Bank for this practice and US Bank ended up paying about two million dollars in settlement to consumers in Minnesota and another two million to numerous other states, where it had committed similar practices.

If you pass SB 2191, that is exactly the kind of marketing scheme our states citizens will be exposed to. We would strike down the customer protections in **current North Dakota Banking statute, which requires the OPT IN, or advanced signature and consent of customers for a bank to sell customer information,** and in its' place impose the much more liberal "OPT OUT" method under Gramm Leach Bliley, for sharing and selling of North Dakota citizens financial information. It's exactly opposite of current North Dakota banking law and opposite of what it should be to protect our states bank customers.

Now, let me share with you the worst part of SB 2191. **The GLB Act applies only to non-public consumer information. The GLB Act does not apply to:**

1. **Commercial Accounts**
2. **Agricultural Accounts**
3. **Public Information**

Therefore, for Commercial and Agricultural accounts in North Dakota, **there will be no protection for ND citizens because there is no federal law that provides that these type of customers even have an opportunity to "OPT OUT". Thus, SB 2191 eliminates all protection under ND State Banking Law for privacy protection for Commercial and Agricultural accounts.** Consequently, if you are a farmer/rancher or a business person doing business with a bank, you **have no protection whatsoever for your financial information under SB 2191.** Any bank in ND that farmers, ranchers and business persons do business with, can sell, share, disclose or give their

private financial information to anyone or any entity, at any time, without these customers knowledge or consent. Furthermore, **even if the farmer, rancher and business person desires to stop the banking institution from disclosing their financial information, under SB 2191 the bank could choose to ignore the request.**

Existing banking law under Chapter 6-08.1, which was enacted in 1985, applies to banks, thrifts, credit unions and savings and loans and provides that **the financial institution has a duty to protect all information unless specifically allowed to be released under one of the 11 exemptions or unless the customer grants affirmative consent.** If SB 2191 is enacted, banks, thrifts and credit unions will have the ability to release information on commercial and agricultural accounts, including account numbers, without even having to disclose this practice in policy or provide any notification to the customer that the information is being released.

Under GLB, Congress specifically provided under Section 507, that state laws are not affected, superceded, or pre-empted if and then only to the extent, that the states laws or rules are **"inconsistent"** with GLB. A state law is **"inconsistent"** and thus **not pre-empted** if it provides **"protection greater than GLB's privacy provisions as determined by the Federal Trade Commission"**. The Commissioner of Banking, Gary Pressler, has a pending petition with the FTC on North Dakota's existing Banking law to ensure that the affirmative consent requirement, or **"OPT IN"**, under current ND banking law, is not and will not be pre-empted by GLB. Mr. Pressler has informed me that he expects to receive a positive response from the FTC any day.

#### **Is North Dakota alone it its' Privacy Guideline?**

One of the arguments raised by the banks is that we must institute GLB guidelines or ND will be all alone. Nothing could be further from the truth. Currently, **4 other states (Alaska, Tennessee,**

Illinois and Vermont) have banking laws like North Dakota's current law (OPT IN). North Dakota is not an island and financial institutions have been operating under different state laws for years.

As we speak, the following states, in their Legislative Assemblies, are considering the adoption of financial protection legislation for the Constituents of their respective states:

1. AZ	HB	2135	7. MA	HB	229	13. PA	HB	85	
2. CA	HB	1289		HB	32	14. SC	SB	204	
	SB	773	8. MI	HB	4198	15. TX	HJR	15	
3. HA	HB	1466	9. MN	HB	579	16. VA	SB	602	
	HB	1559		SB	567		17. WA	HB	2016
4. ID	HB	116	10. MO	HB	850	18. WI	HB	88	
	HB	239	11. NM	HB	750				
5. IN	760	IAC 1-66	12. NY	HB	18				
6. IA	HB	285		HB	4230				
				SB	2330				

#### The Congress is also concerned about GLB and Privacy

On February 13, 2001, Representative Hutchinson of Arkansas along with Representatives Moran (VA), Brady (TX) Granger, Greenwood and Lucas (OK) and Riley, introduced **HB 583**, to establish the Commission for the Comprehensive Study of Privacy Protection. We are seeing a growing movement across America, as more and more people become aware of the liberal privacy provisions in GLB, to limit the terms of GLB and provide consumers a much greater degree of control over how their confidential information is used, shared and sold by Financial Institutions and other businesses. It is easy to see that the **OPT IN** provision of privacy, provides the greatest degree of protection for the person. **OPT IN** only places a burden to get the consent on those institutions that intend to sell or disclose private information to third parties.

North Dakota's current Banking Laws have protected our North Dakota citizens since 1985.

There is no reason at all to change current ND law. The Congress and many of our sister states are

concerned about GLB. There is no need for SB 2191, unless the intent is to take advantage of the private information the banks have obtained from their customers, and the banks intentions are to sell that information to outside non-affiliated companies in order to make more money.

What this committee must determine is, who do we wish to protect; the confidential information of the people of North Dakota or the financial institutions ability to sell and market that confidential information so they can make more money.

It is my sincere hope that this committee will vote to protect the people of North Dakota and vote to kill SB 2191. Let's not strip away the financial privacy protections we have had for the people of North Dakota since 1985.

I will be happy to answer any questions, Mr. Chairman.

Rep Kuiper  
SB 2191

**CHAPTER 6-08.1  
DISCLOSURE OF CUSTOMER INFORMATION**

**6-08.1-01. Definitions. As used in this chapter:**

1. "Customer" means any person who has transacted or is transacting business with, or has used or is using the services of, a financial institution, or for whom a financial institution has acted as a fiduciary with respect to trust property.
2. "Customer information" means either of the following:
  - a. Any original or any copy of any records held by a financial institution pertaining to a customer's relationship with the financial institution.
  - b. Any information derived from a record described in this subsection.
3. "Financial institution" means any organization authorized to do business under state or federal laws relating to financial institutions, including, without limitation, a bank, including the Bank of North Dakota, a savings bank, a trust company, a savings and loan association, or a credit union.
4. "Financial institution regulatory agency" means any of the following:
  - a. The federal deposit insurance corporation.
  - b. The federal savings and loan insurance corporation.
  - c. The national credit union administration.
  - d. The federal reserve board.
  - e. The United States comptroller of the currency.
  - f. The department of banking and financial institutions.
  - g. The federal home loan bank board.
5. "Governmental agency" means any agency or department of this state, or any authorized officer, employee, or agent of an agency or department of this state.
6. "Law enforcement agency" means any agency or department of this state or of any political subdivision of this state authorized by law to enforce the law and to conduct or engage in investigations or prosecutions for violations of law.
7. "Person" means any individual, partnership, corporation, limited liability company, association, trust, or other legal entity.

**6-08.1-02. Exemptions. This chapter does not apply to any of the following:**

1. The preparation, examination, handling, or maintenance of any customer information by any officer, employee, or agent of a financial institution having custody of such information or the examination of such information by an accountant engaged by the financial institution to perform an audit.
2. The examination of any customer information by, or the furnishing of customer information to, any officer, employee, or agent of a financial institution regulatory agency solely for use in the exercise of his duties.

3. The publication of data derived from customer information where the data cannot be identified to any particular customer or account.
4. Any acts required of the financial institution by the Internal Revenue Code.
5. Disclosures permitted under the Uniform Commercial Code concerning the dishonor of any negotiable instrument.
6. The exchange in the regular course of business of customer credit information between a financial institution and other financial institutions or commercial entities, directly, or through a customer reporting agency.
7. The release by the industrial commission, in its capacity as the managing body of the Bank of North Dakota, of either of the following:
  - a. The name of any person who, either directly or indirectly, has obtained financing through the Bank of North Dakota.
  - b. The amount of any financing obtained either directly or indirectly through the Bank of North Dakota.
8. An examination, handling, or maintenance of any customer information by any governmental agency or law enforcement agency for purposes of verifying information necessary in the licensing process, provided prior consent is obtained from the licensee and customer.
9. Disclosure of customer information to a law enforcement agency or governmental agency pursuant to a search warrant or subpoena duces tecum issued in accordance with applicable statutes or the North Dakota Rules of Criminal Procedure.
10. Disclosure by a financial institution to the commissioner of agriculture that it has given a customer notice of the availability of the North Dakota agricultural mediation service.
11. The disclosure by a financial institution to any financial institution or other entity that controls, is controlled by, or is under common control with the financial institution if the financial institution or other entity receiving the information complies with section 6-08.1-03.

**6-08.1-03. Duty of confidentiality.** A financial institution may not disclose customer information to any person, governmental agency, or law enforcement agency unless the disclosure is made in accordance with any of the following:

1. Pursuant to consent granted by the customer in accordance with this chapter.
2. To a person other than a governmental agency or law enforcement agency pursuant to valid legal process.
3. To a governmental agency or law enforcement agency pursuant to valid legal process in accordance with this chapter.
4. For the purpose of reporting a suspected violation of the law in accordance with this chapter.
5. For the purpose of notifying the commissioner of agriculture that a financial institution has notified a customer of the availability of the North Dakota agricultural mediation service.

6. As part of the disclosure made of deposits of public corporations with financial institutions in the security pledge schedule verified by the custodian of securities pursuant to section 21-04-09.

**6-08.1-04. Consent.**

1. No consent or waiver shall be required as a condition of doing business with any financial institution, and any consent or waiver obtained from a customer as a condition of doing business with a financial institution shall not be deemed a consent of the customer for the purpose of this chapter.
2. A valid consent must be in writing and signed by the customer. In consenting to disclosure of customer information, a customer may specify any of the following:
  - a. The time during which such consent will operate.
  - b. The customer information to be disclosed.
  - c. The persons, governmental agencies or law enforcement agencies to which disclosure may be made.

**6-08.1-05. Government access.**

1. A governmental agency or law enforcement agency may obtain customer information from a financial institution pursuant to either of the following:
  - a. The consent of the customer, in accordance with this chapter.
  - b. Valid legal process, in accordance with this section.
2. A governmental agency or law enforcement agency may obtain customer information from a financial institution pursuant to a judicial or administrative subpoena duces tecum served on the financial institution, if there is reason to believe that the customer information sought is relevant to a proper law enforcement objective or is otherwise authorized by law.
3. A governmental agency or law enforcement agency may obtain customer information from a financial institution pursuant to a search warrant if it obtains the search warrant pursuant to the rules of criminal procedure of this state. Examination of the customer information may occur as soon as it is reasonably practicable after the warrant is served on the financial institution.

**6-08.1-06. Suspicion of unlawful conduct.**

1. Nothing in this chapter precludes a financial institution from initiating contact with, and thereafter communicating with and disclosing customer information to, a law enforcement agency when the financial institution reasonably believes that the customer about whom such information pertains:
  - a. Is engaged in unlawful activity; or,
  - b. Is defrauding the financial institution.
2. Conviction of the customer or admission by the customer shall be conclusive of the reasonableness of the disclosure for purposes of this section.
3. The burden is on the financial institution to show that at the time the disclosure was made, the disclosure was reasonable for the purposes of this section.

**6-08.1-07. Cost reimbursement.** Any governmental agency, law enforcement agency, or person requiring or requesting access to customer information shall pay to the financial institution that assembles or provides the customer information a fee for reimbursement of reasonably necessary costs which have been directly incurred by the financial institution. A financial institution must deliver the customer information sought as soon as reasonably possible notwithstanding any dispute concerning the amount of reimbursement due under this section. A separate action may be maintained by the financial institution against the governmental agency, law enforcement agency, or person requesting access for recovery of reasonable reimbursement. The financial institution may not charge the state auditor for customer information requested when performing an audit; however, the financial institution may charge the entity being audited by the state auditor for the information requested.

**6-08.1-08. Liability.**

1. A financial institution, governmental agency, law enforcement agency, or any other person is liable to the customer for intentional violations of this chapter in an amount equal to the greater of the following:
  - a. One thousand dollars.
  - b. Actual damages caused by the disclosure of the customer information.
2. Any financial institution, governmental agency, law enforcement agency or other person that takes any action pursuant to this chapter, relying in good faith on any provision of this chapter, may not be held liable to any person for its actions.

California

\* currently in Judiciary  
Committee and Business  
& Finance  
to be heard March 15

BILL NUMBER: AB 203 INTRODUCED  
BILL TEXT

INTRODUCED BY Assembly Member Jackson

FEBRUARY 9, 2001

An act to add Chapter 2 (commencing with Section 1798.79) to Title 1.8 of Part 4 of Division 3 of the Civil Code, relating to financial privacy.

LEGISLATIVE COUNSEL'S DIGEST

AB 203, as introduced, Jackson. Privacy: financial transactions; personal information.

Existing law prohibits a business entity that performs bookkeeping services from disclosing the contents of any record which is prepared or maintained by the business entity to any person, other than the individual which is the subject of the record, without the express written consent of the person.

This bill would enact the Consumers' Financial Privacy Act. The bill would prohibit a financial institution, as specified, without a consumer's prior written consent, from disclosing or making an unrelated use of the personal information collected by the financial institution in connection with any transaction with the consumer involving any financial product or any financial service or otherwise obtained by the financial institution. The bill would require various disclosures by financial institutions to consumers. The bill would provide for specified civil remedies and the imposition of a civil penalty by a court or the imposition of an administrative fine by a regulatory agency.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Chapter 2 (commencing with Section 1798.79) is added to Title 1.8 of Part 4 of Division 3 of the Civil Code, to read:

CHAPTER 2. CONSUMERS' FINANCIAL PRIVACY ACT

1798.79. (a) This chapter shall be known as and may be cited as the Consumers' Financial Privacy Act.

(b) The Legislature finds and declares all of the following:

(1) The right to privacy is an inalienable right protected by the California Constitution and the United States Constitution.

(2) The right to privacy protects individuals from the unauthorized collection, retention, and dissemination of personal information by business interests.

(3) Individuals have a reasonable expectation of privacy when they provide information to a financial institution.

(4) Inherent in the constitutional right to privacy and the expectation of privacy of information is the right of individuals to control the use, gathering, and dissemination of personally identifiable information.

(5) It is an invasion of privacy for financial institutions to disclose a consumer's personal information without the affirmative written consent of the consumer.

(6) The federal government, through enactment of the federal Gramm-Leach-Bliley Act (P.L. 106-102), has expressly invited states to enact greater protections for the privacy of financial information of their residents.

(c) The Legislature intends all of the following:

(1) The privacy of a consumer's personal information provided to a financial institution by the consumer or otherwise shall be protected.

(2) A consumer's personal information provided to a financial institution may not be disclosed without the consumer's prior written consent.

(3) No financial institution may refuse or limit a consumer's access to any financial product or service for refusing to provide consent or canceling consent to disclosure of personal information provided to the financial institution.

1798.79.1. (a) The following definitions apply to this chapter:

(1) "Affiliate" means any entity that, directly, or indirectly through one or more intermediaries, controls, is controlled by, or is under common control with the other entity.

(2) "Consumer" means an individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes. "Consumer" also includes that person's legal representative.

(3) "Control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of another entity.

(4) "Customer relationship" means a continuing relationship between a consumer and a financial institution under which the financial institution provides one or more financial products or services to the consumer. "Customer relationship" does not include an isolated transaction, or a series of isolated transactions, between a consumer and a financial institution.

(5) "Financial institution" includes a commercial bank, trust company, savings association, credit union, industrial loan company, insurance company, securities brokerage, mortgage lender, or person engaged in the business of lending money.

(6) "Personal information" means personally identifiable information provided by a consumer to a financial institution in connection with any transaction with a consumer involving any financial product or any financial service or personally identifiable information otherwise obtained by the financial institution from the consumer or any other third party.

(7) "Unrelated use" means any use other than a use that is necessary to effect, administer, or enforce a transaction with a consumer in any financial product or any financial service or that exceeds the stated purpose for which the consumer consented to disclosure.

(8) "Written consent" includes consent provided by electronic mail or other electronic means.

(b) A consumer has a protected privacy interest in all of the personal information that he or she provides to a financial institution or that a financial institution otherwise obtains.

(c) A consumer shall have a cause of action for any violation of this chapter.

1798.79.2. (a) A financial institution may not disclose to any affiliate or nonaffiliated third party, or through any affiliate or nonaffiliated third party, or make an unrelated use of, any personal information unless the financial institution receives the consumer's prior written consent for the disclosure or use of the information. The financial institution shall notify the consumer of the

information it wishes to disclose or use, the individual or business entity that will receive the information, and the purpose for the disclosure or use, at the time that it solicits written consent from the consumer. All those notifications shall also clearly and conspicuously state that the financial institution may not refuse or limit a consumer's access to any financial product or service for refusing to provide consent or canceling consent to the disclosure or unrelated use of personal information.

(b) At the time of establishing a customer relationship with a consumer, at the time of the first solicitation for written consent from the consumer, and not less than annually thereafter, all financial institutions shall clearly and conspicuously disclose to the consumer all of the following:

(1) The categories of personal information that are collected by the financial institution.

(2) The policies and practices that the financial institution maintains to protect the confidentiality and security of personal information.

(3) Categories of persons or entities to whom the information is or may be disclosed or who may be permitted to make unrelated use of the information.

(4) The practices and policies of the financial institution with respect to providing consumers with the opportunity to examine and dispute information subject to disclosure or unrelated use by the financial institution or any affiliates or nonaffiliated third parties.

(5) The right of a consumer to refuse or cancel consent to the disclosure or unrelated use of any personal information, and that the financial institution may not refuse or limit access to any financial product or service for exercising that right.

(c) If the financial institution adopts a policy of nondisclosure and a policy prohibiting any unrelated use of personal information, and for so long as the financial institution maintains and observes those policies, the financial institution shall not be required to comply with the annual notification requirements of subdivision (b). In that case, the financial institution shall be obligated to disclose this policy to consumers only once, either at the time of establishing a customer relationship, or through communication with existing customers.

(d) Except as provided in subdivisions (e) and (f), the prior written consent required by subdivision (a) may be a general authorization to cover some or all transactions, provided that:

(1) Any general authorization shall clearly and conspicuously disclose to the consumer the consumer's right to cancel the general authorization at any time, as well as all of the information described in paragraphs (1), (3), (4), and (5) of subdivision (b).

(2) If a consumer consents to a general authorization, a financial institution shall provide a consumer with a written notice of each disclosure or unrelated use that the financial institution makes of the consumer's personal information either within 30 days of disclosure or use, or with the next account statement, billing statement, or other document provided to the consumer by the financial institution if the statement or other document is provided within 60 days of disclosure or use. The written notice shall include the personal information disclosed or used, who received the information, the purpose of the disclosure or use, and the consumer's right to cancel the general authorization at any time.

(3) An individual may cancel any general authorization at any time. Immediately upon cancellation of a general authorization, a financial institution shall be required to obtain the consumer's prior written consent for any and all subsequent disclosures or unrelated uses of information subject to the provisions of this chapter.

(e) A financial institution shall not disclose to any affiliate or any nonaffiliated third party, or through any affiliate or any nonaffiliated third party, without the prior written consent of the consumer, the consumer's account number or similar form of access number or access code for a credit card account, deposit account, checking or savings account, debit card, transaction account, or similar type of account number or access number or code, or the existence of any one or more of these accounts for use in any marketing or commercial purpose, including, but not limited to, telemarketing, direct mail marketing, or marketing through electronic mail or other means.

(f) An affiliate or a nonaffiliated third party that receives from a financial institution the personal information of a consumer shall not, directly or through an affiliate of the receiving party, disclose or make an unrelated use of the information to any other person or entity without the prior written consent of the consumer. An affiliate or any nonaffiliated third party shall be required to directly and independently secure the consumer's prior written consent to disclose or make an unrelated use of personal information.

Prior written consent provided to a financial institution may not include consent for an affiliate or nonaffiliated third party to subsequently disclose or make an unrelated use of personal information of a consumer with any other person or entity.

(g) Subdivision (a) shall not be construed to prohibit the disclosure of personal information without the prior written consent of the consumer in any of the following circumstances:

(1) The disclosure is necessary to effect, administer, or enforce a transaction requested or authorized by the consumer in connection with servicing or processing a financial product or service requested or authorized by the consumer, for maintaining or servicing the consumer's account with the financial institution, or for enforcing a financial obligation of the consumer arising from any transaction with the financial institution.

(2) The disclosure is necessary to protect the confidentiality or security of the financial institution's records pertaining to the consumer, the service or product, or the transaction.

(3) The disclosure is necessary to protect the consumer against actual or potential fraud, unauthorized transactions, claims, or other liability.

(4) The disclosure is made to persons holding a legal or beneficial interest relating to the consumer or acting in a fiduciary or representative capacity on behalf of the consumer.

(5) The disclosure is made to law enforcement agencies to the extent specifically permitted or required under state or federal law.

(6) The disclosure is made in compliance with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by federal, state, or local authorities, or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution.

(7) The disclosure is made to a local, state, or federal agency for child support enforcement purposes.

(8) The disclosure is made to a consumer reporting agency in accordance with the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.) or the Consumer Credit Reporting Agencies Act (Title 1.6 (commencing with Section 1785.1)).

(h) No financial institution may refuse or limit a consumer's access to a financial product or service for refusing to provide consent to the disclosure of personal information provided by the consumer to the financial institution or for canceling that consent.

(i) Every financial institution shall provide a consumer, upon request, with the opportunity to examine all personal information

subject to disclosure or unrelated use, to dispute the accuracy of any of the information, and to require the financial institution to correct information that has been demonstrated by the consumer to be inaccurate.

1798.79.3. (a) In addition to any other remedies available under state or federal law, all of the following remedies, fines, and penalties are applicable to a violation of this chapter:

(1) Any individual may bring an action against a financial institution, or affiliate or nonaffiliated third party, that has negligently disclosed or used personal information in violation of this chapter, for either or both of the following:

(A) Nominal damages of one thousand dollars (\$1,000). In order to recover under this subparagraph, it shall not be necessary for the consumer to have suffered actual damages.

(B) The amount of actual damages, if any, suffered by the consumer.

The court shall award reasonable attorney's fees and costs to the plaintiff if he or she prevails in the action.

(2) Any financial institution, or affiliate or nonaffiliated third party, that violates, proposes to violate, or has violated any provision of this chapter may be enjoined in any court of competent jurisdiction.

(3) A financial institution, or affiliate or nonaffiliated third party, that negligently discloses or uses personal information in violation of the provisions of this chapter shall be liable, irrespective of the amount of damage suffered by the consumer as a result of that violation, for an administrative fine or civil penalty not to exceed two thousand five hundred dollars (\$2,500) per violation.

(4) A financial institution, or affiliate or nonaffiliated third party, that knowingly or willfully discloses or uses personal information in violation of this chapter shall be liable for an administrative fine or civil penalty of not less than two thousand five hundred dollars (\$2,500) but not to exceed twenty-five thousand dollars (\$25,000) per violation.

(5) A financial institution, or affiliate or nonaffiliated third party, that knowingly or willfully discloses or uses personal information in violation of this chapter for the purpose of financial gain shall be liable for an administrative fine or civil penalty not less than twenty-five thousand dollars (\$25,000) but not more than two hundred fifty thousand dollars (\$250,000) per violation and shall also be subject to disgorgement of any proceeds or other consideration obtained as a result of the violation.

(6) Nothing in this subdivision shall be construed as authorizing an administrative fine or civil penalty under both paragraphs (4) and (5) for the same violation.

(b) In assessing the amount of an administrative fine or civil penalty pursuant to paragraph (3), (4), or (5) of subdivision (a), the regulatory agency or court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the following:

(1) Whether the defendant has made a reasonable, good faith attempt to comply with this chapter.

(2) The nature and seriousness of the misconduct.

(3) The harm to the consumer.

(4) The number of violations.

(5) The persistence of the misconduct.

(6) The length of time over which the misconduct occurred.

(7) The willfulness of the defendant's misconduct.

(8) The defendant's assets, liabilities, and net worth.

(c) (1) The civil penalty imposed pursuant to paragraph (3), (4), or (5) of subdivision (a) shall be assessed and recovered in a civil action brought in the name of the people of the State of California

in any court of competent jurisdiction.

(2) Nothing in this section shall be construed as authorizing the imposition of both an administrative fine and civil penalty for the same violation.

(3) The imposition of an administrative fine or civil penalty provided for in this section shall not preclude the imposition of any other sanctions or remedies authorized by law.

Rep Keeper SB2191

<b>THIS SEARCH</b>	<b>THIS DOCUMENT</b>	<b>GO TO</b>
Next Hit	Forward	<a href="#">New Bills Search</a>
Prev Hit	Back	<a href="#">HomePage</a>
Hit List	Best Sections	<a href="#">Help</a>
	Doc Contents	

<a href="#">GPO's PDF version of this bill</a>	<a href="#">References to this bill in the Congressional Record</a>	<a href="#">Link to the Bill Summary &amp; Status file.</a>	<a href="#">Full Display - 4,854 bytes.</a> <a href="#">[Help]</a>
--	---	---	--

**Financial Institution Privacy Protection Act of 2001 (Introduced in the Senate)**

S 450 IS

107th CONGRESS

1st Session

**S. 450**

To amend the Gramm-Leach-Bliley Act to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes.

**IN THE SENATE OF THE UNITED STATES****March 1, 2001**

Mr. NELSON of Florida introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

**A BILL**

To amend the Gramm-Leach-Bliley Act to provide for enhanced protection of nonpublic personal information, including health information, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the 'Financial Institution Privacy Protection Act of 2001'.

**SEC. 2. PROTECTION OF PRIVATE HEALTH INFORMATION.**

Section 509(4) of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(4)) is amended by adding at the end the following:

'(D) The term 'nonpublic personal information' includes health information, defined as any information, including genetic information, demographic information, and tissue samples collected from an individual, whether oral or recorded in any form or medium--

'(i) that is created or received by a health care provider, health researcher, health plan, health oversight agency, public health authority, employer, health or life insurer, school or university; and

'(ii) that --

'(I) relates to the past, present, or future physical or mental health or condition of an individual (including individual cells and their components), the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

'(II) that identifies an individual, or with respect to which there is a reasonable basis to believe that the information can be used to identify an individual.'

### **SEC. 3. OPT-IN FOR SHARING OF INFORMATION.**

Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended--

(1) in subsection (a)--

(A) by inserting 'any affiliate or' before 'a nonaffiliated';

(B) by striking 'unless such' and inserting the following: 'unless--

'(1) the institution provides'; and

(C) by striking the period at the end and inserting the following: '; and

'(2) the consumer to whom the information pertains--

'(A) has affirmatively consented (in writing, in the case of health information, as defined in section 509(4)(D)), in accordance with rules prescribed under section 504, to the disclosure of such information; and

'(B) has not withdrawn such consent.'; and

(2) by striking subsection (b) and inserting the following:

'(b) DENIAL OF SERVICE PROHIBITED- A financial institution may not deny a financial product or a financial service to any consumer based on the refusal by the consumer to grant the consent required by this section.'

## SEC. 4. COMPLIANCE OFFICERS.

Section 503 of the Gramm-Leach-Bliley Act (15 U.S.C. 6803) is amended by adding at the end the following:

`(c) COMPLIANCE OFFICERS- Each financial institution shall designate a privacy compliance officer, who shall be responsible for ensuring compliance by the institution with the requirements of this title and the privacy policies of the institution.'.

## SEC. 5. LIABILITY.

Section 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6805) is amended by adding at the end the following:

`(e) CIVIL PENALTIES- The Attorney General of the United States may bring a civil action in the appropriate district court of the United States against any financial institution that engages in conduct constituting a violation of this title, and, upon proof of such violation--

`(1) the financial institution shall be subject to a civil penalty of not more than \$100,000 for each such violation; and

`(2) the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than \$10,000 for each such violation.'.

---

<b>THIS SEARCH</b>	<b>THIS DOCUMENT</b>	<b>GO TO</b>
<a href="#">Next Hit</a>	<a href="#">Forward</a>	<a href="#">New Bills Search</a>
<a href="#">Prev Hit</a>	<a href="#">Back</a>	<a href="#">HomePage</a>
<a href="#">Hit List</a>	<a href="#">Best Sections</a>	<a href="#">Help</a>
	<a href="#">Doc Contents</a>	

---

Rep Kasper SB2191

<b>THIS SEARCH</b>	<b>THIS DOCUMENT</b>	<b>GO TO</b>
<a href="#">Next Hit</a>	<a href="#">Forward</a>	<a href="#">New Bills Search</a>
<a href="#">Prev Hit</a>	<a href="#">Back</a>	<a href="#">HomePage</a>
<a href="#">Hit List</a>	<a href="#">Best Sections</a>	<a href="#">Help</a>
	<a href="#">Doc Contents</a>	

<a href="#">GPO's FDF version of this bill</a>	<a href="#">References to this bill in the Congressional Record</a>	<a href="#">Link to the Bill Summary &amp; Status file.</a>	<a href="#">Full Display - 3,153 bytes.[Help]</a>
--	---	---	---

**Social Security Number Privacy Act of 2001 (Introduced in the Senate)**

S 324 IS

107th CONGRESS

1st Session

**S. 324**

To amend the Gramm-Leach-Bliley Act, to prohibit the sale and purchase of the social security number of an individual by financial institutions, to include social security numbers in the definition of nonpublic personal information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

February 14, 2001

Mr. SHELBY introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

**A BILL**

To amend the Gramm-Leach-Bliley Act, to prohibit the sale and purchase of the social security number of an individual by financial institutions, to include social security numbers in the definition of nonpublic personal information, and for other purposes.

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

**SECTION 1. SHORT TITLE.**

This Act may be cited as the 'Social Security Number Privacy Act of 2001'.

**SEC. 2. AMENDMENTS RESTRICTING THE SALE AND PURCHASE OF SOCIAL SECURITY NUMBERS.**

(a) IN GENERAL- Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended by adding at the end the following:

**“(f) REGULATION OF THE SALE AND PURCHASE OF SOCIAL SECURITY NUMBERS AND SOCIAL SECURITY ACCOUNT NUMBERS-**

**“(1) PROHIBITION-** Notwithstanding any other provision of this title, no financial institution may sell or purchase a social security number or a social security account number in a manner that violates a regulation promulgated by the Federal functional regulators under paragraph (2).

**“(2) REGULATIONS-**

**“(A) IN GENERAL-** Not later than 6 months after the date of enactment of the Social Security Number Privacy Act of 2001, the Federal functional regulators shall promulgate regulations restricting the sale and purchase of social security numbers and social security account numbers by financial institutions.

**“(B) RESTRICTIONS AND CONDITIONS-** In promulgating regulations under subparagraph (A), the Federal functional regulators shall impose restrictions and conditions on the sale and purchase of social security numbers and social security account numbers that are no broader than necessary--

**“(i) to provide reasonable assurances that social security numbers and social security account numbers will not be used to commit or facilitate fraud, deception, or crime; and**

**“(ii) to prevent an undue risk of bodily, emotional, or financial harm to an individual.’.**

(b) DEFINITIONS- Section 509(4)(A) of the Gramm-Leach-Bliley Act (15 U.S.C. 6809(4)(A)) is amended by inserting ‘, including a social security number or social security account number’ after ‘financial information’.

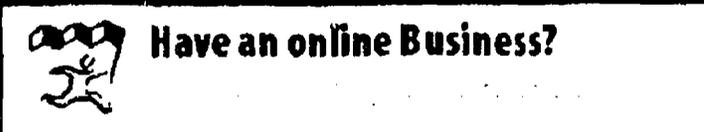
---

<b>THIS SEARCH</b>	<b>THIS DOCUMENT</b>	<b>GO TO</b>
<a href="#">Next Hit</a>	<a href="#">Forward</a>	<a href="#">New Bills Search</a>
<a href="#">Prev Hit</a>	<a href="#">Back</a>	<a href="#">HomePage</a>
<a href="#">Hit List</a>	<a href="#">Best Sections</a>	<a href="#">Help</a>
	<a href="#">Doc Contents</a>	

---

Rep Kasper SB2191

visit the Anonymizer's Sponsors:

	
--	---

LinkExchange

Page loaded anonymously by Anonymizer.com

Sign Up for a Premium Account!

Jump anonymously to this site

Search anonymously for

http://  Go!

URI Encryption Disabled Safe Cookies Disabled Page Delay On Banner Ads On

## Financial Privacy: The Shortcomings of the Federal Financial Services Modernization Act

California Bar Association  
Annual Meeting, San Diego, CA  
Sept. 15, 2000

Presentation by Beth Givens  
Privacy Rights Clearinghouse  
[www.privacyrights.org](http://www.privacyrights.org)  
[bgivens@privacyrights.org](mailto:bgivens@privacyrights.org)

[Note: In the interest of time, a shorter version of this speech was given to the Bar Association. The excerpts that were omitted are marked with brackets.]

I am Beth Givens, director of the nonprofit program the Privacy Rights Clearinghouse, located here in San Diego. We were established in 1992 and have a two-part mission: first, to educate consumers on ways they can protect their privacy; and second, to advocate for privacy protection laws, regulations, and industry practices in public policy proceedings such as legislative and regulatory hearings, as well as in industry conferences.

Our web site contains all of our consumer education publications -- guides on how to get rid of junk mail and telemarketing calls, how to recover from identity theft, medical records confidentiality issues, Internet privacy and the like. The site also contains our public policy writings, such as speeches and legislative testimony.

Some of you may remember when we were a part of the University of San Diego Law School's Center for Public Interest Law. Since 1996, we have been affiliated with the local consumer organization UCAN, the Utility Consumers' Action Network.

The definition of privacy that guides our efforts is that of control. "Privacy is the [ability of individuals] ... to determine for themselves when, how, and to what extent information about this is communicated to others." (Alan Westin, *Privacy and Freedom*, 1967, p.7). Much of what I have to say about the shortcomings of the federal Financial Services Modernization Act, or Gramm-Leach-Bliley, deal with customers' *inability to control* how their financial-related information is used in a wide variety of situations.

My presentation will cover these topics:

- a short explanation of the Gramm-Leach-Bliley Act
- the public opinion landscape -- what the polls are telling us these days about consumers' concerns about threats to their privacy
- the California Legislature's response to this federal law
- what privacy advocates propose as a better approach
- a bit about the political climate in the next two years

#### SUMMARY OF THE FINANCIAL SERVICES MODERNIZATION ACT

The new federal law, the Financial Services Modernization Act, enables three industries to affiliate under one corporate roof -- banking, insurance, and securities. The Act requires that banks and financial services provide an "opt-out" for customers to restrict the sale of personal information to *third parties*. But it gives no ability for customers to restrict the sharing of data between and among *affiliates*.

With the implementation of the Gramm-Leach-Bliley Act, we are looking at a radical change in the way personally identifiable information is collected and used in the marketplace. Think about it. We are talking about the ability of three mega-industries being able to merge their customer information, each of which alone holds extremely sensitive information:

( All of this information can now be merged into a single data base -- without our consent. )

I never assume that people understand the difference between opt-in and opt-out. "Opt-out" means that financial institutions can share or sell customer information without their affirmative up-front consent. If customers do not tell the bank to refrain from selling their

data, such sale will go on indefinitely. "Opt-in" means that the default is set an "no sharing." The customer must provide consent before any personal data is shared.

## THE PUBLIC'S FEARS ABOUT THREATS TO PRIVACY

What is the public opinion landscape? Do consumers really want such three-industry profiles developed without their consent? Polls and recent cases indicate No.

- A 1998 AARP poll found that 81%, or 4 out of 5, consumers opposed internal sharing of customer data by affiliates. Only 10% supported it.
- A 1998 Lou Harris poll found that 78% had refused a company their personal information for privacy reasons. 82% felt they had lost all control of their personal information. Overall, 90% said they are concerned about threats to their privacy.
- A pre-millennium 1999 Wall Street Journal poll found that the number one issue of concern to those surveyed was privacy, outranking even terrorism, education and other burning issues.
- Take a look at the uproar that has greeted the long form of the Census this year.
- Also, look at the controversy that erupted with the merger of Doubleclick and Abacus, when their customer profile data bases were going to be merged without consent. Doubleclick is an Internet ad-placement company that captures the web-surfing patterns of millions of Internet users, on a mostly anonymous basis. It acquired Abacus, a company that compiles personally identifiable information about the mail order catalog purchases of 90 million households. Consumers have responded to the potential merger of the offline Abacus data with the online Doubleclick data with a firestorm of protest that has shaped public policy development and industry actions greatly since then.
- Finally, a recent poll by the Pew Internet and American Life Project found that 86% of Internet users favor the opt-in approach.

( In short, consumers want control over uses of their personal information.) This flies in the face of the weak privacy standards of the Gramm-Leach-Bliley Act.

## WHAT ARE THE CONCERNS? OF THE PRIVACY AND CONSUMER ADVOCATES

Industry representatives claim the privacy provisions of the federal law are far reaching and unprecedented. Granted, the amount of disclosure required of financial services industries *is* unprecedented. But that doesn't take away from the fact that consumers lack either an opt-in or opt-out ability to prevent the sharing of customer data shared between and among affiliates. I believe that the Gramm-Leach-Bliley Act *is* one step forward ... but many large steps backward. Allow me to explain.

Each of these industries -- banking, insurance, and securities -- compiles a tremendous amount of sensitive personal data from the transactions of its customers. Think for a moment about what can be determined about you from your banking and credit card data, especially for persons who use credit cards a great deal and engage in online banking -- our payments for medical services, entertainment and recreation choices, political interests, charities we support, religious affiliation, and so on.

Consider insurance company records. They include your health conditions, potentially from cradle to grave. Life, automobile, and home insurance information are also highly revealing.

Records from brokerage firm accounts also say a great deal -- the extent of your investment assets, whether you are a conservative investor or take risks, perhaps even your affinity for get-rich schemes and your vulnerability to scams.

The sale of data without consent from any of these three industries could result in significant harm to consumers, much more than simply the aggravation of receiving unsolicited telemarketing calls.

\* Note the cases last summer and fall in Minnesota and New York, where their Attorneys General sued U.S. Bancorp and Chase Manhattan respectively for the sale of data to third parties contrary to their own privacy policies. In the Minnesota case, U.S. Bancorp sold customer data -- including account numbers and balances, types of accounts Social Security numbers, and phone numbers -- to a telemarketer, Memberworks. When Memberworks successfully sold a product such as a travel club to a bank customer, it automatically debited the account, which it was able to do because the account number had been provided. Many of those customers were not aware that they had given consent to have their accounts debited.

These are examples of abuses that can occur within a single industry when customer data is sold without consent. Now let's look at what can happen when two major financial services industries are allowed to affiliate -- the banking and the securities industries.

\* In 1998 Nation's Bank was fined nearly \$7 million by the U.S. Securities and Exchange Commission for deceiving many of its bank customers into switching their stable savings into the more risky investments of its affiliated securities company. Many of these customers were elderly. They were not made aware of the implications of such decisions. In fact, many did not realize that they were stepping outside of the relative security of their bank accounts into an environment where they could lose their principal. Many incurred significant losses to their life savings.

At our own hotline, we have seen several cases like the Nation's Bank scenario involving a prominent bank in which unwary seniors were advised to switch their savings to riskier investments, and then incurred losses. Nation's Bank is not an isolated case. And the SEC investigation and fine has not stopped other banks from engaging in similar practices.

Another example of the kind of abuse that can occur when the boundaries between two financial industries are blurred is the sale of lead lists from brokerage customer files, also known as "sucker lists." Fraud investigators for the securities industry are well aware of this practice and the tremendous harm befalling the individuals, mostly elderly, who "bite" on these schemes and often lose everything.

[A securities fraud investigator recently told me about scams perpetrated on the elderly by "fraudsters" who learn they have sizable assets in their bank accounts. "Lists of names of people with liquid assets in the bank are very valuable, especially to fraudulent telemarketers," she told me. She described a lawsuit against a man operating a fraudulent investment business who had a side business of selling 'lead lists.' He was getting about \$200 a name for 'hot' leads. The senior citizens who have ready money in the bank and are lonely too often welcomes the friendly voice over the telephone. The fraud investigator concluded that the ability of banks to freely share such information about their customers with their affiliated securities firm, without the protection of an informed opt-in consent requirement, is a "major disaster waiting to happen."]

Given that backdrop, consumers are now faced with the merger of three industries, with only the most meager of privacy and disclosure requirements involving third parties. Banks and other financial services can share their significant storehouses of customer data with affiliated insurance companies and brokerage firms without any consent required, not even an opt-out.

I consider affiliate sharing to be no different than third party sale in terms of the final results. The fact that a law has been passed enabling the affiliation of these three industries does not somehow magically make the sharing of customer data between and among these industries benign and without harmful effect.

I have so far mentioned the confusion and fraud potentials that can result from affiliate data sharing. But I haven't yet talked about privacy implications of merging customer data across these three data-rich industries. )

\* The profiling opportunities of combining such customer data are enormous. Now we are being told by industry that the kinds of products and services that will be offered as a result of the merger of their financial, insurance and securities data are so beneficial that no consent is required -- not the up-front opt in, or the after-the-fact opt-out. In this rosy scenario, no consideration is given to possible negative and harmful secondary uses of the data. I would submit that the kind of data that will be shared among banks, insurance companies and brokerage firms is equally as sensitive as the kind of data that would have been merged by Doubleclick and Abacus, in fact, for the most part, far more sensitive.

A basic privacy principle -- one that goes back a quarter century and is a cornerstone of the European Union's Privacy Directive -- is the secondary use principle. "Information that has been collected for one purpose shall not be used for other purposes without the consent of the individual."

Let me use an example from the world of supermarket club card data to illustrate secondary use. The Smith's Food chain, headquartered in Utah and operating in the Southwest, has a very successful discount club program whereby data on each and every purchase of card carriers are recorded. In a story documented in the Washington Post, the U.S. Drug Enforcement Agency subpoenaed the club card records of individuals they were investigating. They were not looking for large quantities of the over the counter medications that comprise "speed," as you might expect. But they were seeking large volume purchases of plastic baggies used, presumably, to package the illicit drugs and sell them on the street. You might respond that such a use is socially beneficial. But how many girl scout leaders buy large quantities of baggies to wrap the troop's sandwiches?

What is the moral of this story? Profiling does not always lead the profiler to the correct conclusion.

- Will secondary uses of the rich profiles compiled about customers be found? I think we can count on it. Will customers be able to control which of those secondary uses they would allow? Certainly not within the corporate family of affiliated companies. And with only an opt-out required for third part dissemination of customer data, many consumers might not take the step needed to prevent those disclosures.

I'm currently reading an excellent book about the present privacy policy environment in the U.S. It's Jeffrey Rosen's *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, 2000). Rosen is a professor of law at George Washington University. His main concern is the compilation of bits and pieces of information about us from disparate sources, taken out of context, and then used to form conclusions and make decisions about us. He says:

Privacy ... protects us from being objectified and simplified and judged out of context in a world of short attention spans, a world in which part of our identity can be mistaken for the whole of our identity. (p. 115)

In his book, Rosen frequently discusses the subpoenaing of Monica Lewinski's book purchases from a Washington, D.C., bookstore as an example of how such profiling can harm us. I have no doubt that the rich profiles compiled by merged financial institutions will be highly sought after in civil proceedings like divorces, child custody suits, business lawsuits, and the like, not to mention criminal investigations.

#### THE CALIFORNIA LEGISLATURE'S RESPONSE: OPT-IN LEGISLATION

I've discussed the public opinion environment of the Gramm-Leach-Bliley Act, and I've covered many of the objections of privacy advocates to this far-reaching measure. What was the legislative response?

The federal Act contained a provision enabling states to enact stronger privacy measures. And many state legislatures stepped up the plate with strong opt-in bills -- requiring opt-in

consent for both third party sharing and affiliate sharing. Roughly half the states introduced such bills.

Here in California, we had not one opt-in bill, but three. Remember, we have a strong tradition of consumer protection laws in this state. In addition, we have a strong right to privacy in our Constitution, one that has been interpreted to affect the private sector, as well as the public sector.

The three financial privacy bills were: Assemblymember Sheila Kuehl's AB 1707, Senator Jackie Speier's SB 1337, and Senator Tim Leslie's SB 1372. Leslie's bill is all the more remarkable because he's a Republican and the chair of the Senate Banking Committee. ([www.leginfo.ca.gov](http://www.leginfo.ca.gov))

The bills were somewhat similar. They required these provisions:

- Disclosure by the financial institutions of information collected, what is done with the information, and how it is secured.
- Opt-in consent for both third party and affiliate sharing of customer data.
- The right of access to information and the ability to correct erroneous data.
- An anti-coercion clause, stating that banks cannot condition on the receipt of service with the disclosure of customer information to affiliates and others.
- Penalties for noncompliance, private right of action.
- Of course exceptions were built into these bills for law enforcement access, child support enforcement and the like.

Such provisions are often referred to as the fair information principles – the building blocks of many privacy laws, not only in the U.S., but in the European Union, Canada, Australia, New Zealand, Japan, and Hong Kong.

The common principles are: disclosure, consent, access, correction, security, collection limitation, accountability, and secondary use restrictions. For example the federal Fair Credit Reporting Act of 1970 is based on the fair information principles. So is the federal Privacy Act of 1974.

These principles were first introduced in the U.S. in the early 1970s. They spread to the western European countries and became the foundation for their omnibus privacy laws,

called "data protection" laws. The approach in the U.S. has differed significantly from the direction taken in the industrialized countries. Most countries have adopted omnibus laws, covering all aspects of life, whereas in the U.S. we have adopted sector-by-sector privacy laws. Examples are credit reporting, telemarketing, government records, video rental records, and cable television.

Our approach is characterized as a "patchwork" of laws. We are criticized by European Union (EU) countries for protecting video rental records, for example, more strongly than medical records. I will *not* discuss the protracted struggle between the U.S. and the EU countries over the lower privacy protection standards in the U.S. vis-a-vis the EU Privacy Directive.

Let me return to a discussion of the 2000 legislative session and what happened to the three strong opt-in bills. The short story is they were all killed because of strong and highly orchestrated opposition by the financial services industries. They combined forces nationwide by forming a group called the Financial Services Roundtable. Their representatives appeared at the hearings in all states where opt-in bills were introduced, including California. Even though 15 consumer advocacy organizations formed a loose coalition to support the three bills, we had nowhere near the people-power and funding to launch an effective campaign.

Senator Tim Leslie attempted to convert his bill into an opt-out bill, requiring an opt-out for both affiliate and third party sharing. But that measure did not gain the support of either industry or the consumer organizations.

[Before talking about what we can expect next year, I would like to address the main arguments that the financial industry made against the opt-in approach.

**Business costs:** The first is the cost to businesses of the opt-in approach. Industry representatives state that opt-in is too costly and will put up barriers to businesses that want to merge with each other and reach out to new customers. I ask, costly compared to what? These industries are currently very successful. There is no evidence that their current business models will not succeed in the future. What we are really talking about is that opt-in *MAY* mean their profits won't be as high as they could be if they have to take extra steps to inform customers of their consent actions. And I stress *MAY*. Remember this is the New Economy, the Internet Age.

Industry analysts also claim that the opt-in approach costs significantly more because companies will have to get permission from customers *each and every time* they want to share or sell their information. On the contrary: In an opt in environment, companies will have clear policies that are communicated to all customers in bill inserts, on their web sites, when customers are in one-to-one contact with company staff.

Further, when making the cost argument, industry fails to take account of the huge individual and societal costs that result from fraud and consumer confusion.

In addition, the cost of implementing the required Gramm-Leach-Bliley opt-out disclosure notices is going to be huge. Why would it cost any more to provide notice about the opt-in approach? FYI, I read in one report that banks think it will cost about \$1 per customer to provide them the required notice of the Gramm-Leach-Bliley Act.

Besides, it may be that some cost is to be expected ... in order to be able to use customer data in a merged system ... in order to ensure consumer safeguards ... in order to allow the time for the marketplace to mature. I am not saying opt-in has to be forever. There may be a time when there will be enough consumer awareness to shift to an opt-out model.

**Consumer convenience:** A second industry argument against the opt-in requirement is the inability of affiliated companies to offer convenient and beneficial services to consumers.

Industry representatives have talked about the convenience of one-stop shopping, of merged statements, and of highly customized services. Granted, some customers *are* savvy enough about the pro's and con's of allowing the three industries to safely merge their customer data. But most, I would wager, are not.]

Let's think back to the results of telecommunications deregulation begun 15 years ago. The negative fallout from that process has been considerable consumer confusion and fraud -- for example, slamming and cramming.

I believe the marketplace must be allowed to mature before opt-out can even be considered to adequately safeguard consumer privacy. And given the sensitivity of one's customer data within the financial services industries, I am not sure that opt-out can ever be adequate, even with the most stringent disclosure requirements.

#### WHAT NEXT?

We are now at the end of the legislative year. No strong financial privacy bills made it to the Governor's desk. What can we expect next year and the year after?

Assemblymember Sheila Kuehl, who is expected to win her state Senate race, has said she will re-introduce her opt-in bill.

There has also been talk of a consumer privacy ballot initiative being introduced. But what it would look like is up in the air. If you remember nearly 30 years ago, it was a ballot initiative in 1972 that established our state's constitutional right to privacy in Article 1, Section 1 of the California Constitution. Given the very high poll numbers showing consumer alarm, even outrage, over the loss of privacy, a ballot initiative might have strong public support.

#### CONCLUSION

In closing, having a bank account is a necessity for most individuals. Consumers should not have to trade off their privacy in order to obtain much needed financial, securities, and insurance services. Because of the sensitivity of customer data as well as the potential for the data to be used in ways that are harmful to consumers, it is critical that strong opt-in and disclosure standards be passed into law for both affiliate and third party sharing.

Thank you for your attention.

---

### Privacy Rights Clearinghouse

[More About Us](#) | [Fact Sheets](#) | [Speeches & Testimony](#)  
[Privacy Links](#) | [Cases](#) | [About Our Book](#) | [Identity Theft Resources](#) | [E-mail](#)

**HOME**

([www.cnie.org](http://www.cnie.org)) monitors the state of online marketing to children. The Electronic Privacy Information Center ([www.epic.org](http://www.epic.org)) features news, a comprehensive list of organizations, newsletters, and conferences covering privacy issues. And Junkbusters ([www.junkbusters.com](http://www.junkbusters.com)) provides detailed advice and software to help the computer-savvy user fend off junk mail, telemarketing calls, faxes, e-mail, and web banner ads.

**Priorities for privacy policy.** There's an important role for public policy in curbing the excesses of privacy invasion on the Internet's nearly lawless frontier. A good starting point would be to codify common principles of privacy protection that the U.S. and the member states of the European Union agreed to in 1980. That accord affirmed these five consumer privacy rights:

**Notice.** Consumers should be clearly informed, in agreed-upon language, how data are collected, how they will be used, and to whom they might be disclosed.

**Choice.** Consumers should be able to limit the use of information beyond what's essential to complete a transaction. There are two principal ways to do this: Web sites can permit them to "opt in," or explicitly grant advance permission to share information. Or they can put the onus on consumers to "opt out" if they don't want information shared. For sensitive medical and financial data, Consumers Union believes that the "opt in" approach is the preferred standard.

**Access.** Consumers should have a timely and inexpensive way to view data gathered about them and to contest its accuracy.

**Security.** Organizations that gather data from consumers must reasonably ensure that the information they keep is secure against loss or unauthorized access.

**Enforcement.** As evidenced by the half-hearted application of current voluntary standards, self-regulation is not off to an impressive start. Meaningful enforcement must be accompanied by stiff sanctions that punish privacy violators. So far, regulators have selectively investigated privacy infringements but will have to step up those efforts as more transactions are conducted on the Internet.

Implementation of these principles is only beginning to get under way. The Clinton administration has proposed legislation to ensure the privacy of medical records, and federal regulators are just starting to put standards for safeguarding the privacy of financial records and transactions in place. Clearly, there's a long way to go.

# Financial privacy

Rep Kasper  
SB 2191

**New megabanks are trying to make sense out of your dollars—and you. Here's how to keep your money matters private.**

"A bum?" asks the caption below a picture of a man sporting a scruffy beard and clad in jeans, a rumpled jacket, and sandals. "A billionaire," answers the caption when you turn the page and see a photograph of the man's back, a bag stuffed with money slung over his shoulder.

This ad is from Trans Union, one of three major consumer credit-reporting agencies, and it hits a familiar point: Appearances can be deceiving, but facts don't lie. It also underscores another reality given new urgency lately: Financial-services companies—banks, brokers, insurers, credit-card issuers, and the credit bureaus that serve them—now have at their disposal more-intimate facts about what consumers earn, spend, borrow, own, and invest in than ever before.

The sweeping new financial-services deregulation law that was passed late last year tore down the barriers dating back to the Great Depression that barred commercial banks from selling insurance and investment products, and blocked insurers and investment companies from owning banks. But by allowing these once arms-length companies to band together under one corporate umbrella, the new law also dismantled the barriers that kept information about consumers securely compartmentalized. Deregulation and the powerful technology that financial institutions now use are revealing just how few legal protections consumers really have when it comes to keeping information about their personal finances private.

Today affiliated companies are able to share within their common corporate family—and, in some cases, even with third parties—what they know about you. The

new license to share data raises new concerns for consumers. For example, might the fact that you run up large monthly charges on your credit card result in your having to pay more for an auto loan? Could the health condition that disqualified you from getting an insurance policy also prevent you from having a mortgage approved?

Each contact with the parent company can potentially influence the kind of service you get as a client, the products you're offered, and what you pay for them—or whether you're seen as a desirable customer at all. We'll explain what that can mean for you personally and for consumers in general, and what you need to know to ensure that information about your finances is used to your benefit.

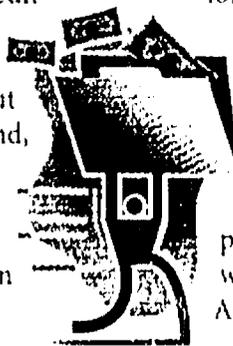
## THE NEW POWERHOUSES

Even before the deregulation law passed, a wave of mergers and acquisitions was transforming the financial landscape. Among the biggest deals:

▶ Citibank, the nation's second-largest commercial bank, teamed up with Travelers Group, the big insurance holding company that had previously merged with the prominent investment firm Salomon Smith Barney. The new entity, Citigroup, has more than 100 million customers worldwide.

▶ North Carolina's NationsBank joined forces with giant BankAmerica to form Bank of America, a financial-services network that now reaches one-third of all U.S. households.

▶ First Union Corp. expanded far beyond its Charlotte, N.C., base to swallow up Philadelphia's CoreStates Bank, Richmond, Va.-based Wheat First Securities, a brokerage house, and The Money Store, a so-called subprime lender that specializes in extending high-cost credit mainly



lower-income consumers.

► Fleet Financial, once a midsize New England bank, has merged with Bank-Boston, acquired the investment firm Robertson Stephens, and bought the discount brokerage Quick & Reilly to form FleetBoston Financial. The new financial-services giant serves more than 20 million customers in some 20 countries.

► Charles Schwab, another big discount broker, has expanded into a full-service financial supermarket, culminating early this year in the purchase of U.S. Trust, a prestigious New York bank catering to a mostly affluent clientele.

These new alliances have yet to integrate their full range of product offerings or to put in place the data-mining systems that will enable them to target new products with laser accuracy to individual consumers. And there's no doubt consumers can ultimately look forward to many potential new conveniences. For example, bank customers will be able to consolidate their checking and brokerage accounts into a single monthly statement. And preferred clients can look forward to more-customized service, better product choices, and tailored financial-planning advice.

But privacy experts such as Joel Reidenberg, a law professor at Fordham University in New York, and consumer groups including Consumers Union, publisher of CONSUMER REPORTS, worry that the dissolving boundaries between financial-services companies and their ability to link huge databases might be a source of potential harm as well. They caution that banks and finance companies can disseminate sensitive information about their customers to third parties without their permission. Financial institutions, too, can use their databases to consign some consumers to second-class status. They could also decide to withhold services from customers they don't find sufficiently profitable to serve. Indeed, Reidenberg points out, the ability to mine customer data is one of the major forces driving the creation of these large financial conglomerates. What the consumer is offered, he says, will be based on his or her information profile.

There has already been some high-profile evidence that these concerns are justified. For example:

► In January Chase Manhattan Bank settled charges levied by the New York state attorney general that the bank was selling sensitive information on some 20 million

customers, including credit-card numbers and account balances, to direct-marketing firms such as Cendant and BrandDirect, companies that sell memberships in travel and gardening clubs. Chase agreed to stop sharing such information in the future.

► In Minnesota, U.S. Bancorp, under investigation by that state's attorney general, agreed to end its sales of information about its customers' checking and credit-card accounts to outside marketing firms.

These cases and other suspected instances of unwarranted data sharing have led state attorneys general in New York, Illinois, and other jurisdictions to launch investigations into how financial companies, including credit-card issuers, maintain consumer privacy.

#### **BIG RISKS, WEAK PROTECTIONS**

These early instances of the inappropriate use of personal data point to deeper problems that consumers may face as the pace of financial consolidation picks up. But they

## **This bank is lawfully allowed to share some information with our affiliated banks and companies even if you request us to limit the sharing of information.**

also demonstrate how few legal safeguards currently exist to forestall potential abuses.

**Mingling data on health and wealth.** It's standard practice for life-insurance companies to require that policy applicants undergo a physical exam to determine whether the insurer will issue a policy and at what price. To fill in gaps about the prospective client's medical history of poor health, obesity, or a problematic driving record, insurers also routinely consult an industry-sponsored database in Westwood, Mass., called MIB (for Medical Information Bureau), which maintains detailed profiles on millions of Americans.

Information that's gathered with a consumer's consent, for the legitimate purpose of letting an insurer know the potential risks it faces when it writes a policy, can harm the customer a second time if it's passed along to an affiliated company that makes credit decisions. These adverse health data could be used to deny a loan or lower a credit

limit. Currently no regulations prohibit an insurer from sharing information about your medical condition with any affiliated lending arm. Insurance-industry executives such as Herb Perone, spokesman for the American Council of Life Insurers, downplay reasons to be concerned, since, he says, companies refrain from sharing medical information for marketing purposes. The Clinton administration is currently drafting rules intended to put formal limits on the use of private medical data, and we'll examine medical privacy more fully in an upcoming issue.

**Disclosure loopholes.** Under the newly passed bank-deregulation guidelines, financial-services firms are required to inform you of their privacy policies when you open a new account or take out a loan. And the companies will have to distribute copies of their policies once a year. Some of those policies candidly state that the company is willing to share information about you freely. For example, the current privacy statement from Wells Fargo states, "We are lawfully allowed to share some information with our affiliated banks and companies even if you request us to limit the sharing of information. It is our policy to share this information... to the fullest extent permitted by law."

Likewise, your bank, insurer, or broker is required by the new banking law to notify you before it shares information about you with another company, and to allow you to opt out if you don't want others to have it. But there's a big escape clause. If your financial institution creates a marketing alliance with another financial company—say, a link between your bank and an unrelated insurance company—it is not required to give you the opportunity to have your information withheld. You'll be able to keep your name off the company's marketing lists—but only for nonfinancial products.

**Data "redlining."** Federal law prohibits banks from denying credit to any consumer based on the borrower's race, gender, religion, or national origin. It also forbids "redlining," a term derived from the once common practice of bankers and mortgage companies to draw a red line on maps marking off neighborhoods where they would not lend. But no law prevents financial institutions from using other types of data to discriminate between desirable borrowers and less profitable consumers the institutions want to avoid. In fact, some companies—including Equifax, the credit-

reporting bureau with headquarters in Atlanta, and HNC Software, based in San Diego—sell programs to help financial companies do this. Among other things, one Equifax product, called Decision Power, helps guide tellers and other point-of-sale bankers through scripted sales pitches that draw on a customer's profile to persuade the account holder to buy extra products.

Financial institutions use customer data to differentiate between those who present a poor credit risk and those to whom they are willing to extend only subprime loans at higher interest rates. But out of that effort to determine which customers are credit-worthy, a more insidious form of data redlining recently surfaced. Lenders profit handsomely by extending loans to subprime borrowers who diligently pay off their high-cost credit. In fact, so lucrative is this business that some creditors, including many subprime lenders and large credit-card issuers, were said by consumer groups and regulators to be withholding from the credit-reporting bureaus documentation of a borrower's good payment history that might qualify them for more-advantageous loan terms from a competitor. Troubled by the prospect that this recent practice may deny millions of borrowers the opportunity to lower their credit costs, federal banking regulators earlier this year pressed lenders to end the withholding of helpful information, and the creditors appear to have complied. Lenders we contacted, including Household Finance, The Money Store, and First USA, said they are now reporting all information to credit bureaus.

**Your dossier for sale.** Your privacy might also be at risk in new ways when information about you does find its way into the files of the credit bureaus. For years banks, credit-card issuers, and other lenders have turned to the industry's big three players, Equifax, Experian, and Trans Union, for reports detailing consumers' loan-repayment history. They used these as a basis for determining whether a potential borrower is a credit-worthy risk. But now the credit bureaus are expanding beyond their core business. They have begun mining their detailed databases and selling information to retailers and other businesses, who use it to identify which consumers are the likeliest prospects to buy their goods and services.

Although the federal Fair Credit Reporting Act bars them from selling your financial records to anyone who lacks a legitimate

business reason for having them, the credit bureaus can and do tap their databases to create detailed demographic profiles based on the nonfinancial information they have stored: age, address, occupation, and the like. Looking to expand its profiling capabilities, Equifax recently announced that it was buying the direct-marketing business of R.L. Polk & Co., a company that maintains records of consumers' lifestyles and purchase patterns of 105 million households.

In March the Federal Trade Commission took an important step toward blocking the credit bureaus' sale of consumer profiles by ordering Trans Union's PerformanceData subsidiary to stop the practice. But Trans Union says it does not divulge confidential credit material and, claiming the FTC's order infringes on its commercial free-speech rights, has vowed to fight the directive.

#### RECOMMENDATIONS

Clearly, a high priority for consumers is finding the appropriate level of regulatory oversight to ensure that financial-services deregulation delivers its promised benefits without compromising sensitive data in customer accounts. Congress has directed the Federal Reserve Board, the FTC, the Securities and Exchange Commission, and other agencies with regulatory oversight to draft new privacy rules, which are due out in final form this month. In addition, some 20 states are weighing whether to tighten privacy laws within their jurisdictions. Among federal guidelines being discussed is a rule that bans financial institutions from releasing account numbers to outside marketers such as travel clubs, as well as more-explicit requirements that financial-services companies provide clients with regular disclosure of their privacy policies.

But Consumers Union believes the proposed regulations don't go far enough. Banks and other financial-services providers would still be able to share personal information freely across all of their subsidiary companies, even when an account holder expressly requests otherwise. Consumers must now "opt out" of having their information shared with nonfinancial companies. But a better policy would be to prohibit this information sharing unless consumers "opt in," expressly agreeing to receive marketing information, whether from outside marketing firms or from affiliates of a financial-services company.

It's uncertain whether comprehensive legal protections will be put in place anytime soon. You can protect your own privacy by taking these steps:

Scrutinize privacy policies carefully. Don't take out a loan, sign an insurance contract, or open a bank, brokerage, or credit account until you've ascertained what the financial institution intends to do with your information. And if you

already have an active account, pick up a copy of the company's privacy statement the next time you visit a branch or log on to its web site. One of the better policies we've seen is Bank of America's, though it too has its problems. B of A states that it will honor requests to be kept off marketing lists and will not provide any customer information to third-party institutions. It even lists how individuals can get off outside mailing lists for preapproved offers of credit. But the bank retains the right to share private information about its customers among its affiliates.

**Keep accounts separate.** Sure it's convenient to have all of your financial-service needs met by a single provider. But if it makes you uneasy knowing that your mortgage lender might be able to review the records its insurance affiliate keeps on you or see regular monthly updates of your credit-card charges from the charge-card unit, consider keeping different accounts at different institutions.

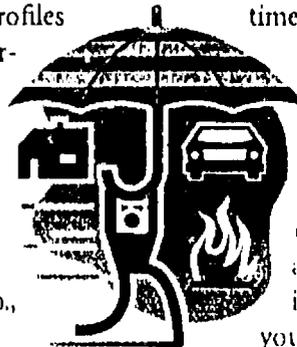
**Opt out.** Your best privacy defense for now is to follow the procedures your financial-service providers establish. You should be able to remove your name from any unaffiliated marketing lists and, wherever possible, keep it out of the hands of its subsidiary companies. You can also have your name removed from lists generated by the major credit-reporting bureaus for preapproved credit offers by calling 888 567-8688, a toll-free number that processes opt-out requests for all three agencies. Or you can write to each of the companies. Here are the addresses:

#### Options

Equifax Inc.  
P.O. Box 740123  
Atlanta, Ga. 30374-0123

Experian Consumer Opt Out  
P.O. Box 919  
Allen, Texas 75013

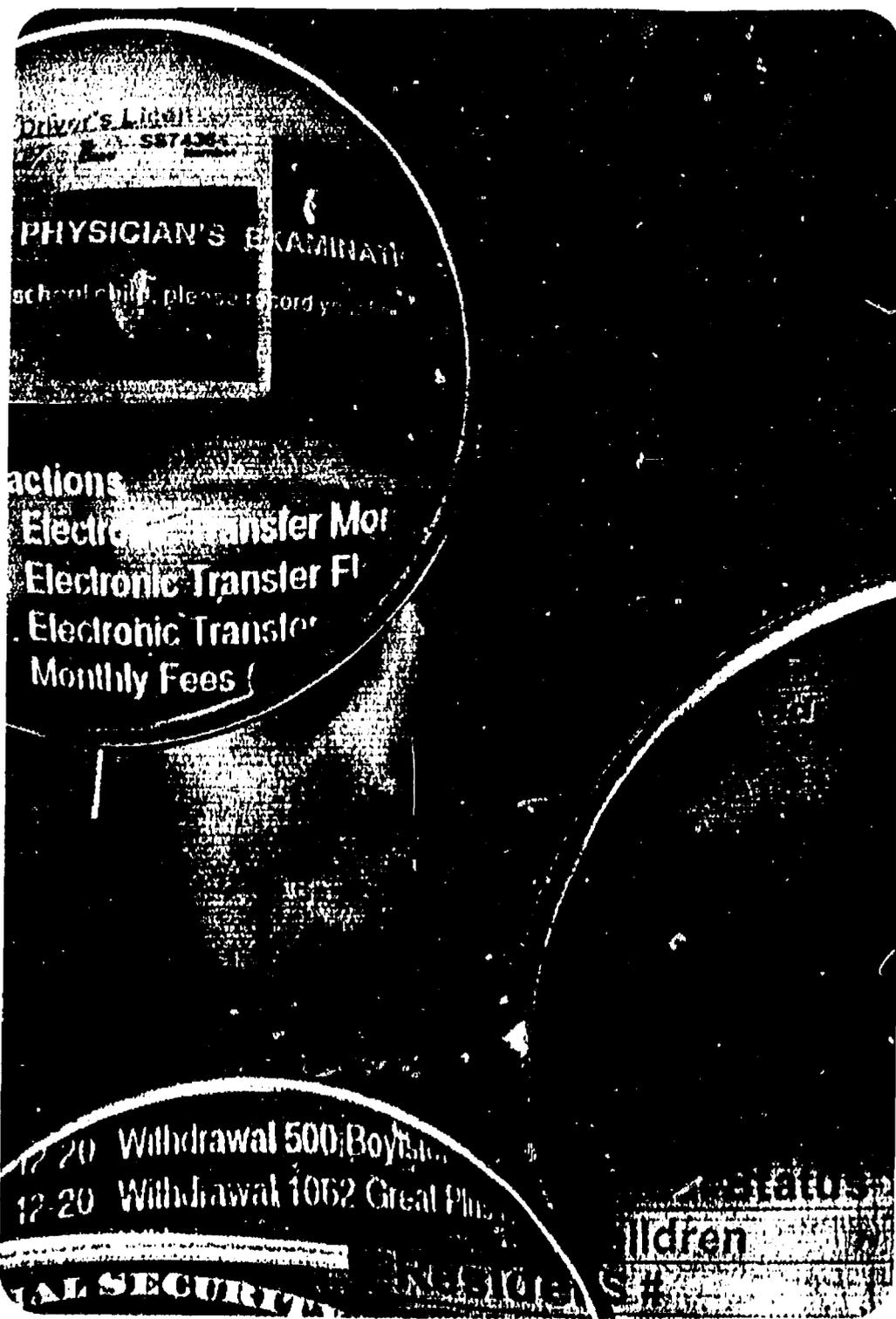
Trans Union LLC's Name Removal Option  
P.O. Box 97328  
Jackson, Miss. 39288-7328



Rep Kupper SB2191

# SELLING IS Getting PERSONAL

Marketers say that having personal data about you helps them deliver the goods you want. But are there risks in the way they get the goods on you?



**W**ithin the walls of Compaq Computer's Advanced Technology Lab in Cupertino, Calif., sits one of the company's most ambitious new undertakings: the Zero Latency Engine. A computational powerhouse, the ZLE packs two rooms with blinking monitors and disk drives the size of Sub-Zero refrigerators. Its prodigious memory bank can store a staggering 6.4 quadrillion bits of data.

This behemoth looks as if it could run a space station, but its purpose is much more down-to-earth: to help businesses crunch reams of data about you and tens of millions of other consumers. Built initially for large telephone companies, financial institutions, and dot-coms, the ZLE vacuums up data on customer transactions as they happen, analyzes the information, and with "zero latency"—or no delay—shunts the results to as many as 100,000 service representatives or out to the Internet. Perhaps its most important role, says Dave Collins, a Compaq spokesman, will be to "generate a profile that suggests things you might want or should have"—a new calling plan, perhaps, or garden shears to go with the lawn mower you just ordered.

Time was, businesses relied on mass marketing rather than sophisticated machines to move the goods. But in recent years, another movement has emerged to take its place alongside mass persuasion: customer-relationship management, that is, marketing to consumers one-on-one. With the help of speedier, more capacious computers, companies can now aggregate an unprecedented amount of information about you. Then, with the help of sophisticated statistical software, businesses can mine the data and compare your preferences and spending

PHOTO ILLUSTRATION BY RALPH MERCER

habits with those of similar customers to home in on products, services and incentives that are especially attractive to you.

Most of us have become accustomed—or resigned—to the idea that businesses are gathering and storing personal information about us. And instead of bombarding consumers indiscriminately with offers for everything under the sun, this personalized marketing can result in sales pitches and promotions for products you might actually want to buy. That's the theory, anyway, and so far there's scant evidence that merchants' collection of information has seriously harmed consumers.

But there are nagging worries. Ari Schwartz, a policy analyst for the Center for Democracy & Technology, a privacy group, points out that data gathering and sharing often occur without our direct knowledge or consent. He and other privacy advocates say there is potential for abuse. Leaks from company databases—whether intended or accidental—could release damaging or embarrassing tidbits to neighbors, strangers, or even criminals. And profiling techniques that allow companies to cosset their best customers could be used just as effectively by those who would zero in on vulnerable consumers—the elderly, the poor, and the unsophisticated—offering them inferior goods or predatory deals. Current state and federal laws enacted to protect consumers from abusive forms of prying are patchy at

best. (See "Holes in the Privacy Safety Net?" on page 20.)

In this report, the last in our three-part look at privacy in the new information age, we focus on how merchants hope to use your personal data to sell to you. You'll see what information businesses collect—often surreptitiously—and how marketers intend to use the data in automated sales campaigns. "The Empires of Info," on page 18, describes the doings of the nation's largest data-collection companies. You'll find tips on how you can limit the use of your own information. And in "Protecting Privacy in the Information Age," below, we outline a public agenda to beef up standards. (For our take on privacy online, see "Big Browser Is Watching You," published in May 2000. "Who Can See Your Medical Records?" was published in the August issue.)

#### GETTING TO KNOW YOU

Dealing with customers as individuals is the aim of all information gathering by businesses, says Bruce Kananoff, CEO of Accelerating 1 to 1, a Stamford, Conn., consulting group. Just as the neighborhood butcher used to know what cuts of meat shoppers liked, a huge company can cater to customers by having its computers store their preferences. Says Kananoff: "It's doing business the old-fashioned way."

Perhaps. But the neighborhood druggist, grocer, banker, and car dealer didn't sell

what they knew about their customers to other companies thousands of miles away. Businesses these days, however, are amassing and sharing an enormous volume of data of all kinds.

Transaction records are collected by merchants you patronize and stored in data warehouses. Good records, of course, can be helpful to consumers who call in to get service, request a part, or complain. But companies also tap such data to market new products, encumbered by few restraints on how they may be used. This year, for example, a Denver federal-court judge ruled that even though telephone-call records are private under federal law, U S West could use those of its customers to pitch extra features for long-distance or wireless plans.

Warranty cards, surveys and sweepstakes entries invite you to fill out lengthy questionnaires about your hobbies, finances, and personal medical conditions. The fine print might advise you that you need not supply any information to qualify for a prize or receive warranty protection, but it won't tell you that your answers will be sold to a large data-collection company. These sources can yield a rich trove of information unavailable through other means. And because such information is "self-reported," explains Jennifer Barrett, a privacy officer for Acxiom, a leading information vendor, there is nothing to block its resale. This information, freely given, allowed Acxi-

## PROTECTING PRIVACY in the information age

Throughout our three-part investigation into consumer privacy, we kept running up against the same questions over and over again: Is privacy a "right?" Who "owns" information about you? Is some data—about your health or finances—so sensitive that its use by others should be strictly circumscribed?

These aren't new issues, of course, but they take on a new urgency as commerce moves swiftly into the Internet age, ratcheting up the volume of personal information that's gathered and exchanged. Here are the priorities for setting guidelines that Consumers Union backs:

**Clear privacy disclosures—and the right to say "no."** Consumers need unambiguous, plain-English statements explaining what information is collected, for what purpose it is used, and with whom it is shared. The fact that personal-

ly identifiable information is traded or exchanged with third-party partners or affiliates should be presented prominently. The disclosures should also provide a simple way for consumers to opt not to have their personal data used for marketing purposes.

**Regular privacy audits.** Independent, periodic audits by third-party experts are needed to verify that data are securely stored and used only for the purposes disclosed, that access is restricted to employees authorized to handle them, and that training programs are in place to guard against leakage or corruption.

**Opt-in requirements.** Organizations that collect and maintain financial and medical records should be obligated to get their customers' specific authorization—or, in privacy parlance, have them "opt in"—before data can be used for any purpose

beyond the needs of the immediate transaction. Consumers should retain the right to inspect files for errors and correct them. Federal legislation introduced separately by Sen. Richard C. Shelby (R. Ala.) and Rep. Edward J. Markey (D. Mass.) would provide those needed opt-in assurances.

**A potent public-sector privacy watchdog.** The exchange of often-sensitive data across government agencies and the hodgepodge of rules governing access beg for intelligent oversight. Recent investigations undertaken by the General Accounting Office of the federal government's own privacy policies and practices underscore the need for coordination and restraint. In 1999, the Clinton administration appointed an official to coordinate privacy issues, but Congress and the next administration should strengthen the office with meaningful enforcement powers.

iom to compile a database of 20 million unlisted phone numbers, which it makes available to law-enforcement agencies and to companies that provide individual reference services to lawyers, private investigators, and large employers.

**Public records**—real-estate documents, court filings, and birth, marriage, divorce, and death certificates—are routinely stripped off computer tapes and sold by state governments to individual reference services as well as to marketers. Even church and school alumni-directory information falls within the category of publicly available data.

**Reverse-append procedures** allow a retailer to learn more about a customer—even about a one-time visitor to a store. Trans Union, the credit bureau, for example, retrieves a customer's name and address if a merchant submits a credit-card number. (Experian and Equifax, the two other credit bureaus, stopped the practice after the Federal Trade Commission [FTC] banned it

in the early 1990s, but Trans Union continues to fight the decision in court.)

**High-tech appliances**—computers, cell phones, and personal digital assistants—draw in even more information to target advertising and offers. "Cookies" and other tracking software implanted on your computer hard drive when you log on to a web site track where you surf online. Other programs can monitor conversations in chat rooms. For example, iLux Corporation, a vendor of marketing software, suggests in its promotional literature that merchants set up online communities—say, for mothers of teenage girls. Then, "as mothers start to discuss appropriate clothes for an upcoming school dance, the site can list offers of both local retailers and cyber-boutiques." Marketers also hope to take advantage of tracking chips in cell phones and PDAs to find out where you are and to beam information to you about nearby stores and restaurants.

The quest for more customer informa-

tion has been fueling mergers and alliance among companies that can profit from each other's data. The Financial Modernization Act, passed by Congress last year, allows alliances among banks, insurance companies, and brokerage houses, which facilitate more information sharing. And online data collectors have married their enterprises to "real world" information providers. Cogit.com, an online marketing-services firm, teamed up with Equifax, which has information on 106 million households. Together, they can monitor who's visiting a web site, identify common characteristics, and enable the site operator to use that information to attract similar customers.

#### DIGGING FOR DOLLARS

Even a minuscule bit of data can be gold to a merchant who uses data-mining software. David Diamond, president of Catalina Marketing, a St. Petersburg, Fla., firm that operates customer loyalty programs for 14,000

## THE OF INFO

These companies have your number—and your address, ZIP code, income level, and hobbies, too. The large data providers listed here generally sell marketers lists of potential new customers or supplement lists of current customers with additional data. They also supply a wide array of analytic and clerical services, data-mining current lists, updating phone numbers and addresses, and so on. In

#### COMPANY

#### PRODUCTS

##### Axclom—Conway, Ark.

Founded in 1969, Axclom provides consumer data and database marketing services through offices in the U.S., Europe, and Australia. Sales in 1999: \$998 million.

**InfoBase** The "largest collection of U.S. consumer, business, and telephone data available in one source" for database or file enhancement, analytical services, or list rental. Consumer data include demographic and lifestyle profiles. **AbillTec** Software that allows clients to use transaction data to personalize offerings to customers.

##### Equifax—Atlanta

One of the three leading credit-reporting agencies, Equifax strengthened its marketing services by acquiring the Consumer Information Systems database from Polk, another data company, earlier this year. Sales in 1999: \$1.0 billion.

**Lifestyle Selector** Data compiled from product-registration cards on household characteristics and leisure activities of 38 million consumers. **High-Tech Connect** Information from surveys and product-registration cards on over 30 million computer and software owners and online-service subscribers. **Outdoor Database** Information derived from boat, vehicle, and aircraft registrations and state hunting and fishing licenses on demographic, recreational and lifestyle activities for over 26 million consumers. **TotalList XL** Data on more than 106 million U.S. households, including lifestyle preferences.

##### Experian—Orange, Calif., and Nottingham, England

Owned by The Great Universal Stores, a British conglomerate, Experian is one of the three major credit bureaus and supplies credit reports and database marketing services. Sales in 1999: \$1.5 billion.

**National Consumer Data Base** Demographic and geographic information on over 95 percent of U.S. households. **BehaviorBank** Lifestyle information through surveys completed by 28 million households. **Insource** Demographic, psychographic, and behavioral data from public and self-reported sources representing 95 percent of U.S. households. **Connexion** Telemarketing data on more than 90 million households.

##### Harte-Hanks—San Antonio

Originally a West Texas newspaper company, now one of the largest database services providers in the U.S., Canada, Europe, South America, and the Pacific Rim. Sales in 1999: \$830 million.

**National Consumer Database** Has lists of over 350 demographic, psychographic, purchase behavior, auto-related, and census attributes. **Shopper ID Numbers** taken from personal checks, credit cards, drivers licenses, and such to help retailers identify customers at point of sale.

##### KnowledgeBase Marketing—Chapel Hill, N.C.

Acquired by Young & Rubicam for \$175 million last year, the company provides e-commerce and direct-marketing services from eight cities in North America.

**AmeriLINK** Data on 200 million individuals, including income, phone numbers, number and ages of children, occupation, and whether family has a credit card. **InTarga** Sorting of a company's prospects and customers into clusters that identify lifestyle behavior and purchase characteristics.

##### PerformanceData/Trans Union—Chicago

A division of the credit bureau, it claims "one of the largest compilations of consumer information outside of the federal government."

**PerformanceBase** Demographic and financial information on 140 million adults. **MasterFile** Lists of over 180 million adult consumers along with household data on each record. **Direct Response Buyers** Information on the activities of 45 million direct-response buyers. **Home Owner Data** Lists of homeowners, with individual-level information on mortgages and home-equity amounts.

supermarkets across the U.S., recalls one chain that searched customer purchase data to find low-fat-food buyers who never bought potato chips. The company then offered them a coupon for a new brand of low-calorie chips. "The response rate was 40 percent," Diamond says, "much better than the 1 or 2 percent you get from a coupon sent in the mail."

Merchants can get much more personal than that, however. From Experian, Acxiom, or some other large data provider, they can purchase an "overlay" of information that customers may have never meant them to have—ages, occupations, what they read, what they earn, and what they own. Then, says Bern Carey, director of the Center for Data Insight at Northern Arizona University, marketing analysts take the data for a spin through statistical software programs to identify their best and worst customers.

Overlays can help companies pinpoint new customers, too. Say a data-mining pro-

## HOW CU uses customer data

Like nearly all publishers, Consumers Union engages in database marketing and has established policies to protect the private information of its customers. We do not rent our mailing list, though we do exchange names and addresses of subscribers with other publishers and nonprofits whose use of such lists passes review of CU's senior management. We currently engage Experian to help us maintain our marketing database and to enhance it with supplemental demographic data. This information is used to assist us in our marketing and fundraising campaigns.

We publicize our opt-out policy in each issue of CONSUMER REPORTS, describing how readers may request that their names not be released to other mailers. And we adhere to guidelines for use of customer names set forth by the Direct Marketing Association. We use information gathered from subscribers who respond to our surveys, polls, or questionnaires only in aggregated form as source material for CONSUMER REPORTS articles and never for marketing purposes.

ject reveals that a company's most profitable customers live within 50 miles of its stores, have incomes between \$50,000 and \$75,000, own their own homes, have teenage children, and recently received a new bank card. The firm could then go to KnowledgeBase Marketing, in Richardson, Texas, and ask for

names of people who fit those criteria from its data bank of 200 million individuals.

All these techniques come into play in the rapidly expanding call-center industry, which currently employs nearly 1.6 million workers. The newest twist in telemarketing, says Keith Dawson, editor of *Call Center News*, is so-called inbound centers, where operators take orders, field complaints, open and close accounts—and, increasingly, sell additional products. "You've got people on the phone already," Dawson says. "So why not try to sell them something?"

Here's how the system works: Say you call into your bank-card company to complain about a fee. An IVRS (interactive voice response system) asks you to key in your account number. Within microseconds, says Dawson, the computerized telephony system can size up from transaction data whether you're a valued customer or a chronic late payer. If the machine likes you, an operator will answer quickly. If not, you'll be kept dangling. The person who ultimately takes your call sees a pop-up screen displaying information about you—that you have kids or like to travel, facts derived from the purchased overlays. The operator may also see a grade that indicates how valuable a customer you are and a churn rate—a prediction of how likely you are to switch your account to another card company. If you are a well-heeled spender who might switch, the operator, following what's become standard practice among creditors, will probably waive your fee. If you're not, she won't. The operator's computer may also have a "next product" recommendation for a college loan program or a travel club.

### KEEPING WHAT'S PRIVATE, PRIVATE

A tangled skein of laws, regulations, and business practices provides some protection

their published privacy policies, all say they comply with federal, state, and local laws in gathering and disseminating information. All comply as well with the Direct Marketing Association's privacy policies by notifying consumers of their right to have their names withheld from information exchanges and honoring requests to be removed from mailing lists.

#### WHO BUYS

#### POLICIES RESTRICTING USE OF DATA

Telemarketers, retailers, e-commerce companies, direct-mail marketers.

Signs fair-use agreements with customers and may require submission of mailing pieces and sales literature. Collects no specific information on children.

Financial-services companies, utilities, retailers, automotive firms, and telecommunications companies.

Fair Credit Reporting Act restricts access to individual personal-credit records to potential lenders and employers with express consent of consumer. Service agreements with customers are audited for compliance.

Retailers, direct-mail firms, utility and telecommunications companies, collection agencies, employers screening job candidates.

Fair Credit Reporting Act restricts access to individual personal-credit records to potential lenders and employers with express consent of consumer.

Financial-services, pharmaceutical, consumer-electronics, publishing, and retailing companies.

Collects and uses "only data pertinent for direct marketing and analytic purposes," counseling its customers on their responsible use. Requires some employees to sign confidentiality agreements.

More than 200 clients in energy, financial services, health care, technology, and retailing.

Binds clients to fair-use agreement contracts and monitors clients' sales pitches by seeding lists with "dummy" records. Collects no individual credit-card or specific merchant-transaction data, credit-reporting information, medical records, or "other sensitive information."

Finance companies, particularly home-mortgage lenders, retailers, restaurants, casinos, publishers, catalog companies, nonprofits, utilities, and ad agencies.

Credit-bureau and insurance reports go only to subscribers making credit offers to consumers. Abbreviated financial and demographic information can be used by all marketers.

against the sharing and misuse of personal information. For now, perhaps the strongest force that keeps information you give one merchant from going to another is competition. It's not to Amazon's advantage, after all, to let detailed data on its customers' book-buying preferences escape to Barnes & Noble. Still, problems abound.

**Murky accountability.** Laws may not apply to a company that is a secondary purchaser of information. When Ronald and Donna Pakkala, a Pennsylvania couple, were rejected for a mortgage, for example, they found that the bank relied on a report compiled by First American Credco from Experian, Trans Union, and Equifax. Their attempt to challenge the information was rebuffed by First American, which claimed it wasn't a credit bureau under the Fair Credit Reporting Act, merely a reseller of information, and thus not responsible for its accuracy. The FTC ruled that First American was covered by the law, but how far the agency's ruling extends is still unclear.

**Careless and intentional misuses.** Not every company is cautious about the data it keeps. Last year, Minnesota Attorney General Mike Hatch charged that U.S. Bancorp illegally sold credit-card numbers and checking-account balance information to MemberWorks, a \$330 million-a-year direct-marketing company that sponsors discount shopping clubs. MemberWorks then used the information to bill Bancorp customers for annual membership fees, even though many people complained that they had not authorized such charges. Within the past year, without admitting wrongdoing, both companies settled, agreeing to pay fines and change their business practices.

**Weak internal controls.** Even when companies establish policies to keep customer data private, information can trickle out. Lawrence Ponemon, who audits companies' privacy programs for PricewaterhouseCoopers, found that only 19 percent of financial institutions surveyed complied with their own privacy policies. Leaks, he says, can be accidental. One worker at a subsidiary of a credit bureau Ponemon audited sold a diskette packed with consumer data to somebody who called in and requested it. "She simply didn't know it was wrong," he says.

**Ambiguous assurances.** Information about its customers is a valuable corporate asset, and when a company is sold or goes bankrupt, customer data can wind up where it was never intended to go. The

## HOLES in the PRIVACY safety net?

If you're worried about your privacy, don't look to the U.S. Constitution to protect you. It contains no explicit guarantees. Federal-court decisions do recognize privacy rights in such intimate personal areas as marital relations, reproduction, and child rearing. As Joel Reidenberg, a law professor at Fordham University, points out, other personal information is guarded by an assortment of laws—most with serious omissions—passed to protect particular types of data.

LAW (listed by date of enactment)	WHAT IT DOES	LOOPHOLES
Federal Trade Commission Act, Section 5 (1935)	Prohibits deceptive or unfair trade practices.	Difficult to prove unfairness or deception in information.
Fair Credit Reporting Act (1970)	Prevents credit bureaus from disclosing personal information except for specified purposes: credit granting, insurance, and employment. Gives consumers the right to view and correct records.	Credit bureaus can sell information to marketers offering "preapproved" credit and insurance deals.
Family Educational Rights and Privacy Act (1974)	Prohibits release of students' school records without permission.	Students have no redress, though schools can lose federal funds.
Cable Communications Policy Act (1984)	Protects cable-television viewing information from being resold.	Cable companies can sell mailing lists of subscribers.
Video Privacy Protection Act (1988)	Bars video stores from disclosing customers' specific video selections unless consumers opt in to such disclosures.	Video stores can release categories of films rented unless consumers opt out.
Driver's Privacy Protection Act (1994)	States must get consumer's permission before selling Department of Motor Vehicle records.	Numerous exceptions allow resale of data to marketers.
Telecommunications Act (1996)	Prohibits telephone companies from selling call records without consent.	Companies may use call records to sell customer more services.
Children's Online Privacy Protection Act (1998)	Requires web-site operators and online services to obtain parents' permission before collecting information from minors.	Applies only if the web site targets children or has knowledge that person registering is a minor.
Graham-Leach-Bliley Act, Title V (1999)	Bars financial institutions from sharing customer information with marketers without consumer's consent.	Banks may share data with insurance companies, brokerages, and other affiliates without consumer's permission.

problems surfaced conspicuously with the demise of e-tailer Toysmart. When this once high-flying dot-com encountered financial troubles earlier this year, it took out an ad in *The Wall Street Journal* offering to sell its database containing identifiable information on some 250,000 names. Later, the company's creditors forced it into bankruptcy. Because Toysmart had pledged to customers not to sell or share their information, the FTC sued for misrepresentation. Toysmart settled with the agency, agreeing to sell the data only to a company engaged in a similar business that pledged to keep the data private. The bankruptcy judge, however, vacated the settlement until a buyer appears.

### RECOMMENDATIONS

**In a data-hungry world,** where you must give up information to buy a house or car, there's no way to ensure total privacy. Nevertheless, you can put some limits on what businesses collect.

**Withhold.** You needn't fill out surveys you get with warranty cards; you don't lose

any legal rights as long as you keep your receipt. Simply mail in a proof of purchase with your name and address to ensure that the manufacturer notifies you if the product is found defective. Second, don't register at web sites until you've read the privacy policy and established that you are comfortable with how your information will be used.

**Opt out.** If you're concerned, write the major data companies and ask to be removed from their lists. To get off all marketing lists, call 212 768-7277 or write the Direct Marketing Association's Mail Preference Service P.O. Box 9008 (mail), Box 9014 (phone), Farmingdale, N.Y. 11735.

**Shield yourself.** If you're sensitive about being tracked on the Internet, set your browser to notify you before it accepts cookies. The Internet is a public venue with eyes all around. Anything you buy or say can be linked to your computer or to you. Today, consumers enjoy no more privacy sitting in front of a terminal in their own homes than they do when they venture out to the local mall. Ⓢ

Rep Kasper SB2191

## Research Wire

Financial Services

Home

NewsWire

Banking

Brokerage

Lending

ECP&amp;P

ATM &amp; EFT

Internet  
Technology

Web Links

Advertising

Contact Us

## Bank Privacy Notices On Web Not Up To Gramm-Leach-Bliley Standards

(August 24, 2000) Two-thirds of all U.S. banks' online privacy notices do not meet the requirements of the Gramm-Leach-Bliley Act because they do not disclose the personal information they collect from consumers, according to a survey by New York City-based PricewaterhouseCoopers' BetterWeb program.

Title V of the Gramm-Leach-Bliley Act requires that specific privacy and security measures be in place by financial institutions voluntarily by November 13, 2000. The Act becomes mandatory on July 1, 2001.

In addition to learning that 65% of U.S. banks' online privacy notices do not disclose the categories of personal information they collect, the BetterWeb survey shows that more than two-thirds (67%) of sites do not state what information they disclose with affiliates and nonaffiliated third parties, such as direct marketing companies. Only 9% of sites disclosed categories and examples of the parties with whom non-public personal information is shared, for example, from a loan application or a credit report. None of the sites reviewed disclosed their practices with respect to nonpublic personal information of former customers.

The banking industry recognizes the importance of disclosing privacy policies to consumers as almost all (98%) of the sites reviewed provide a clear and conspicuous privacy policy. Only one site had a privacy policy that was difficult to locate. The majority of bank sites do not disclose the categories of nonpublic personal information collected from consumers, nor the categories and examples of information that are disclosed with affiliates and nonaffiliated third parties.

Some 65% of sites make no mention of the categories of personal information that they collect from consumers. Only 26% of the sites partially meet the requirement. More than two-thirds (67%) of sites do not state what information they disclose with affiliates and nonaffiliated third parties; 30% partially meet this requirement.

Categories and examples of affiliates and nonaffiliated third parties to whom nonpublic personal information is disclosed must also be included in a company's privacy policy. While companies attempt to address this issue, the privacy policies provided are generally not in sufficient detail to meet the requirement. Only 9% of the sites disclose categories and examples of these parties, for example, information they collect from loan applications or credit reports; 17% do not mention with whom nonpublic personal information is shared; 74% partially meet the disclosure requirement.

Financial institutions must also state their practices regarding disclosing nonpublic personal information about former customers. This includes the categories of nonpublic personal information disclosed and categories of affiliates and nonaffiliated third parties to whom it is disclosed. None of the sites disclose their policies regarding former customers. The banking regulations require that companies provide an explanation of a consumer's opt-out rights, as well as an explanation of a reasonable method through which consumers may opt-out of having their information shared with third parties. Of the 34 sites that state that they disclose information with third parties, less than half (14 sites) disclose consumers' right to opt out and the means to do so. Of the 14 sites, nine provide a reasonable means of doing so, defined as either check-off boxes on relevant forms, a reply form, electronic form to be e-mailed or an electronic process at the bank's Web site, or a tollfree number. All 14 sites provide an opt-out mechanism that would be available to consumers at all times.

The regulations also require financial institutions to inform consumers about policies and procedures with respect to the protection, confidentiality and security of nonpublic personal information. Only 54% of sites disclose both who has access to nonpublic personal information as well as whether security practices and procedures are in place to ensure the confidentiality of that information; 16% do not disclose information to meet this requirement; 31% only partially meet this requirement.

Title V of the Gramm-Leach-Bliley Act (applies to any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust or other financial accounts or relationship with the institution. Under the Act, the federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission and the Federal Trade Commission, in consultation with state insurance authorities, were required to issue regulations implementing the provision of Title V of GLBA by May 12, 2000. The regulations require financial institutions to provide initial and ongoing privacy policy notices to customers.

*Copyright © 2000. This content is the property of Faulkner & Gray.*

Re: Kupper SB2191

Please visit the Anonymizer's Sponsors:



**Have an online Business?**

BannerNetwork  
Microsoft  
**bCentral**

(Choreography)

Page loaded anonymously by Anonymizer.com

**Sign Up for a Premium Account!**

Jump anonymously to this site

Search anonymously for

http://

Go!

URI Encryption Disabled    Safe Cookies Disabled    Page Delay On    Banner Ads On

**Fact Sheet 24: Protecting Financial Privacy**  
**DRAFT REVIEW COPY 12/14/00: We invite your input.**

Copyright 2000. Utility Consumers' Action Network.  
 Released December 2000

This copyrighted document may be copied and distributed for nonprofit, educational purposes only. The text of this document may not be altered without express authorization of the Privacy Rights Clearinghouse. This fact sheet should be used as an information source and not as legal advice. PRC fact sheets contain information about federal laws as well as some California-specific information. Laws in other states may vary. But in general, our fact sheets are applicable to consumers nationwide.

**Privacy Rights Clearinghouse**  
 1717 Kettner Ave., Suite 105  
 San Diego, CA 92101  
 Voice: (619) 298-3396  
 Fax: (619) 298-5681  
 E-mail: [prc@privacyrights.org](mailto:prc@privacyrights.org)  
<http://www.privacyrights.org>

---

**Protecting Financial Privacy in the New Millennium:  
 The Burden Is on You**

Used to be, your bank handled your checking and savings accounts. You visited your insurance agent for life, health, auto, or homeowner's insurance. And, if you wanted to "play the market," you called your stock broker. Recent federal legislation has changed all that. The Financial Services Modernization Act (also known as the Gramm-Leach-

Bliley Act or GLB Act, 15 U.S.C. §§6801-6831) now allows banks, insurance and brokerage companies to operate as one. The consolidated companies have been aptly dubbed "financial supermarkets."

The way you conduct your financial affairs may be forever changed. However, information about you kept in the files of financial institutions is now, and always has been, some of the most sensitive personal information imaginable. Surprisingly, prior to GLB, there were few restrictions on a financial institution's ability to share or even sell your personal information. Title V of GLB gives you some minimal rights to protect your financial privacy. *But the burden is on you to assert your rights.*

### **What privacy rights do I have under GLB?**

GLB requires that your financial institution give you notice of three things:

- **Privacy Policy:** Your financial institution must tell you the kinds of information it collects about you and how it uses that information.
- **Right to Opt-Out:** Before your information can be shared or sold to a third party, you must be given the right to "opt-out," that is to inform your financial institution that it cannot share or sell your information
- **Safeguards:** Financial institutions are required to develop policies to prevent fraudulent access to confidential financial information. These policies must be disclosed to you.

Information about your financial institution's privacy policy, your right to opt-out, and its safeguards will likely be included on a single notice. The notice is usually referred to as an "opt-out notice." Although "opt-out notice" is the term used throughout the GLB Act and the regulations implementing the law, we prefer the term "privacy notice" as more descriptive of the important rights contained in the notices. Also, opt-out is contrary to the "opt-in" approach preferred by most consumer and privacy advocates. Opt-in would prohibit a financial institution from sharing or selling your data if you did not give your affirmative consent. With opt-out, you give your implied consent by failing to return the notice.

### **Will the privacy notice come from my bank?**

Yes. And if you have active accounts with a brokerage house or insurance company, you will receive a privacy notice from these institutions as well. In addition, the Federal Trade Commission (FTC) has taken a broad view of the term "financial institution" in its privacy regulations. This means you may also receive privacy notices from companies you would not consider to be financial institutions such as payday loan companies and travel agents. For this reason, it is particularly important, at least in the next few months, to carefully review all preprinted notices received in the mail or via a company's web site.

### **When will I receive the privacy notices?**

GLB became effective in November 2000. Banking and other federal agencies with oversight of financial institutions have finalized regulations, which, in effect, interpret and fill in the details of the law. In addition, since insurance is regulated by the states and not the federal government, the National Association of Insurance Commissioners (NAIC) has developed model rules for states to use in carrying out the privacy protections of GLB. All financial institutions must be in full compliance by July 1, 2001. This means that you will begin to receive these notices as early as mid-November 2000. Most likely, you will begin to receive them starting in early 2001 through June 2001.

You should receive a notice from every financial institution where you have an ongoing customer relationship. As noted above, you may receive notices from companies where you were not even aware that you had an existing relationship. The American Bankers Association has estimated that the average household will receive about eighteen notices.

### **Will the privacy notice be in writing?**

Generally, yes. Verbal notice alone is not allowed. However, if you do business with a financial institution online, notice on an Internet web page may be sufficient so long as the notice is "clear and conspicuous." For example, an Internet notice should prompt you to scroll down the page in order to view the entire notice or include a drop down menu which draws your attention to the privacy notice. You must *agree* to receive the notice by electronic means and must *acknowledge* having received it.

### **Will the privacy notice be separate from other notices?**

The law does not require that you receive a separate notice of the financial institutions' privacy policy, your right to opt-out, or the institution's policy regarding safeguarding confidential information. There is no standard form so the notice may come in a variety of ways. The exact format is left to the discretion of the financial institution. The law requires only that the notice be "clear and conspicuous" and "designed to call attention to the nature and significance of the information contained" in the notice. Notices may, for example, be mailed along with your account statements. Your privacy notice may also be included with other notices that you are required to receive, for instance, in a mutual fund prospectus. *Remember: if you do not want your financial institution to share or sell your confidential information, the burden is on you to recognize the notice and follow the opt-out instructions.*

### **Can I shop around for a privacy policy I like before opening an account?**

You may certainly ask a financial institution you're thinking of doing business with for a copy of its privacy policy. However, you are only *entitled* to the notice if you are either an existing customer or at the time you establish a "customer relationship" with a financial institution. After that, you are entitled to receive a notice annually. A "customer relationship" means a continuing relationship. You have only a "consumer relationship" if you have an isolated transaction with a financial institution. One example would be an

ATM withdrawal. A "consumer" is entitled to notice of the financial institution's privacy policy only if it intends to disclose information to nonaffiliated third parties.

**I have a joint account with a spouse/friend. Do both of us have to "opt-out" to prevent information from being shared or sold?**

To be safe, probably yes. A financial institution is only required to send a notice to one of the parties to a joint account. It is up to the financial institution to decide how to treat an opt-out notice from one of the parties to a joint account. The financial institution's policy regarding joint accounts should be included in its privacy notice to you. A single notice may also be sent when a financial institution has a "customer relationship" with more than one person in a single household.

**What about closed accounts?**

Initial and annual notices must inform you of the financial institution's policies regarding disclosures of information from closed accounts. Financial institutions are not required to send you a privacy notice if your account is closed. However, if you have an existing account and you opt-out, that is you return the notice saying you do not want your information disclosed, your opt-out election would continue even after you closed the account. If at a later time you decide to open another account with that same financial institution, you would receive another initial privacy notice, which would apply only to data about your new account. You may choose to opt-out of the second account, but your decision with regard to the first account will not change unless you change it.

**How long do I have to opt-out?**

You are entitled to a "reasonable" time to respond before your personal data can be disclosed. Generally 30 days is considered a "reasonable" time to opt-out when notices are sent by mail. When you agree to accept notice via the Internet, you must respond to the notice 30 days after you acknowledge you received it. If you have an isolated transaction, which means you have only a "consumer relationship" with a financial institution, you may be required to decide whether to opt-out at the time of the transaction. For example, if an ATM screen posts a privacy policy and opt-out notice, you must elect at that time whether you want to opt-out. Failure to do so would mean that the financial institution could share or sell your personal data any time after that.

**Do I have to write a letter for every account?**

No. Your financial institution is required to give you a "reasonable" means to exercise your opt-out rights. Requiring you to write individual letters is not considered "reasonable." A formal response should be included with the notice such as a form with check-off boxes or a simple reply form. An e-mail form may be used if your request is processed via the Internet. A toll-free telephone number may also be used for customers to call and opt-out. However, financial institutions are not required to provide pre-paid postage.

### **Can I opt-out by verbally telling my broker or banker?**

No. You must opt-out using the procedure the financial institution establishes, as long as it is reasonable. Again, the burden is on you to follow the procedures set out by your financial institution. Failure to do so could result in disclosure of information you would not tell your best friend.

### **Do I have only one chance to opt-out?**

Your right to opt-out is continuing. If you fail to return the initial opt-out notice or an annual opt-out notice, your financial institution may sell or share your personal data after a "reasonable" time, usually 30 days. If you later decide you want to keep your financial institution from disclosing your personal data, you always have the right to opt-out. It goes without saying, however, that information that is disclosed before you opt-out is already "out there."

### **Will the privacy notice say exactly what information about me can be disclosed?**

The law and regulations require only that your financial institution give you notice of the *categories* of information it collects and the *categories* of information that may be sold or shared with a third party. Financial institutions are also required to give specific examples of the kinds of information included in each category, but this is by no means an exhaustive list of the data that may be disclosed.

The privacy notice may tell you that your financial institution collects and may disclose information obtained from you from account applications and give examples such as your name, address, Social Security number, assets and income. You should assume from such a statement that any other information you provide on an account application could be collected and disclosed. Depending on the nature of the application, other information might include former addresses, debt level, mortgage payments, income other than salary such as child support payments, and much more.

### **Is there any kind of information that can't be disclosed?**

GLB and federal regulations only specifically prohibit financial institutions from disclosing "... an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer." This simply means that a financial institution can sell your personal data to a telemarketer, for example, but it cannot sell the means by which your account could be accessed.

GLB contains no prohibition against the disclosure of particularly sensitive data such as that pertaining to your health status. However, you may have greater rights to protect health information under the laws of your state. For example, California recently passed a law that makes it a crime for an insurance company to sell information to a financial

institution for the purpose of granting credit (AB 2797 in the 2000 legislative session, California Civil Code 56.26). The information flow in this case is only restricted one way. This law does not cover information that flows from a financial institution to an insurance company.

The federal Health and Human Services Department (HHS) is also working to issue regulations covering privacy of medical information. (See [www.healthprivacy.org](http://www.healthprivacy.org).)

### **Where does a financial institution get its information?**

A financial institution may receive information directly from you when, for example, you fill out an application for a new account. Information about you may also be compiled based upon your transactions with that financial institution or its affiliates. This may include information about how you use your credit card, your account balances, late payments and much more. Information may also be collected from nonaffiliated third parties, consumer reporting agencies, or public records.

Consider the amount and kinds of information you supply just to a financial institution that may sell insurance, bank products, and/or securities. Combine this with the information available from other sources, and virtually any detail of your financial affairs, health status, spending habits, lifestyle purchases, political affiliations, religious contributions, and more can be collected by your financial institution. Unless you formally object, it can be shared or sold with few exceptions.

### **What kinds of companies can get my personal information?**

The privacy notice you receive from your financial institution does not have to tell you the names of any specific companies or organizations that may buy or receive your personal information. Again, only the *categories* of companies have to be disclosed to you. Your financial institution may sell your personal information to other financial services providers, one example of which could be an insurance company. Other *categories* of companies that could receive your information might be non-financial service providers such as retailers, direct marketers, or nonprofit organizations.

### **Can I stop my financial institution from sharing my personal information with its affiliates?**

GLB does not place any restrictions on your financial institution's ability to share your personal information with its affiliates. You do, however, have a right under the Fair Credit Reporting Act (FCRA) to opt-out of certain limited information sharing by affiliates. The FCRA right to opt-out includes only "application information" which you provide when, say, filling out an application for credit. Your "transaction and experience" information can still be shared with affiliates without your consent. Such information can be highly sensitive, as explained above. For more information about your ability to opt-out under the FCRA, see PRC Fact Sheet 6, How Private is My Credit Report, at: [www.privacyrights.org/fs/fs6-crdr.htm](http://www.privacyrights.org/fs/fs6-crdr.htm).

### **Why would my financial institution sell my sensitive personal data?**

The financial industry exerted significant influence on Congress to avoid giving consumers affirmative privacy rights, or the right to opt-in to sharing or selling personal financial information. (The right to opt-in means that a financial institution could not share or sell your data without your prior consent.) This same influence was used on the state level when states attempted to pass laws more favorable to consumers. The industry maintains that this "free flow of information" is good for consumers and good for business; companies can market products and services more freely and give consumers information about products they might not otherwise have known to exist. Seldom is the word "sell" used when the industry refers to its handling of confidential financial information.

The reality is that there are profits to be made from the sale of data about individuals. Not all financial institutions engage in this practice. A financial institution's privacy notice to you will state if its practice is not to sell personal information to third parties.

### **May I sue my financial institution for violating my GLB privacy rights?**

No. GLB does not contain what is called a private rights of action, that is the ability of a citizen to go into court and sue for violations of a law. Your only recourse is to complain to one of the seven federal agencies that have jurisdiction over financial institutions under GLB. The seven agencies are identified below along with a description of the kinds of financial institution each oversees. If you have a complaint about an insurance product, contact the National Association of Insurance Commissioners (NAIC, cited below) for the insurance commission in your state.

Each agency has enforcement authority under GLB for the area of financial services it regulates. Enforcement authority means that you can complain to the agency, the agency may investigate your complaint, and may bring a court action or administrative case against the company. The agency cannot represent you and cannot give you legal advice on your particular complaint. Still, it is important to complain to the appropriate federal agency or your state insurance commission because customer complaints represent one of the government's primary sources of information about industry practices.

### **What are the most important things I can do to protect my financial privacy?**

The single most important thing you can do to protect your financial privacy is to carefully read all information that comes from a financial institution. Study the institution's privacy policy. If it causes you concern, return the opt-out notice within the specified time.

Remember, you have very little ability to prevent a financial services company from sharing your customer data with its affiliated companies. The privacy provisions of GLB only pertain to unaffiliated third parties. You would not, for example, be able to prevent your bank from sharing your customer data with its affiliated insurance company or



Washington, D.C. 20552  
(202) 906-6000

**Office of Comptroller of the Currency (OCC)**. The OCC is an agency of the U.S. Department of Treasury. This agency charters, regulates and supervises all national banks as well as the federal branches of foreign banks.

OCC  
Customer Assistance Group [www.occ.treas.gov](http://www.occ.treas.gov)  
1301 McKinley St., Suite 3710  
Houston, TX 77010  
(800) 613-6743

**National Credit Union Administration (NCUA)**. The NCUA regulate and conducts examinations of federal credit unions, which are nonprofit, cooperative financial institutions owned and run by members.

NCUA  
1775 Duke Street [www.ncua.gov](http://www.ncua.gov)  
Alexandria, VA 22314  
(703) 518-6330

**Securities and Exchange Commission (SEC)**. The SEC oversees the nation's equity markets which includes stock exchanges, stock option exchanges, broker-dealers, associated persons of broker-dealers, and investment advisors.

SEC  
Investor Education & Assistance [www.sec.gov](http://www.sec.gov)  
450 Fifth St., N.W.  
Washington, D.C. 20549  
(202) 942-7040

**Federal Trade Commission**. The FTC investigates consumer protection and consumer fraud matters that are not specifically within the jurisdiction of another federal agency such as the SEC. The FTC's consumer protection jurisdiction includes debt collection, credit reports, lending, telemarketing, credit repair services and much more. To file a complaint with the FTC's Office of Consumer Protection, write, call, or contact the agency online:

Federal Trade Commission  
CRC-240 [www.ftc.gov](http://www.ftc.gov)  
Washington, D.C. 20580  
(877) FTC-HELP (877-382-4357)

**Insurance companies.** To find the address and telephone number of the Insurance Commission in your state, write, call, or connect online with the National Association of Insurance Commissioners:

**NAIC**  
2301 McGee Street, Ste 800 [www.naic.org](http://www.naic.org)  
Kansas City, MO 64108-2604  
(816) 842-3600

#### **Relevant Laws**

- Title V of Financial Services Modernization Act (GLB), 15 U.S.C. §§6801-6831
- Fair Credit Reporting Act (FCRA), 15 U.S.C §1681 *et. seq.*

#### **GLB Privacy Regulations**

FTC: *Privacy of Consumer Financial Information*, 16 C.F.R. Part 313; 65 Federal Register 33645 (May 24, 2000). [www.gpo.gov/su\\_docs/fedreg/a000524c.html](http://www.gpo.gov/su_docs/fedreg/a000524c.html)

SEC: *Privacy of Consumer Financial Information* (Regulation S-P). 17 C.F.R. Part 248; 65 Federal Register 40333 (June 29, 2000). [www.sec.gov/rules/final/34-42974.htm](http://www.sec.gov/rules/final/34-42974.htm)

OCC; FDIC; Federal Reserve; OTS (Joint Regulations): *Privacy of Consumer Financial Information*; 12 C.F.R. Part 40; 65 Federal Register 35161 (June 1, 2000). [www.occ.treas.gov/fr/cronolog.htm](http://www.occ.treas.gov/fr/cronolog.htm) (65 Federal Register 35161)

NCUA: *Privacy of Consumer Financial Information*; 12 C.F.R. Parts 716 and 741; 65 Federal Register 31722 (May 18, 2000). [www.bankinfo.com/051800.txt](http://www.bankinfo.com/051800.txt)

---

#### **Privacy Rights Clearinghouse**

[More About Us](#) | [Fact Sheets](#) | [Speeches & Testimony](#)  
[Privacy Links](#) | [Cases](#) | [About Our Book](#) | [Identity Theft Resources](#) | [E-mail](#)

# WRITTEN TESTIMONY IN SUPPORT OF SENATE BILL 2191

---

GREG TSCHIDER, ND CREDIT UNION LEAGUE

Chairman Berg and Members of the Senate Industry, Business and Labor Committee, I am Greg Tschider and I represent the North Dakota Credit Union League, and I am submitting this written testimony in support of Senate Bill 2191.

With the passage in 1999 of the Gramm-Leach-Bliley Act ("GLB"), credit unions in North Dakota have been placed in a dilemma regarding customer information disclosure. Are North Dakota credit unions subject to GLB or the existing North Dakota law or both? Are state chartered credit unions treated differently than federally chartered credit unions? At this point there are no answers.

The Banking Department has requested clarification from the Federal Trade Commission, however, if the FTC grants a preemption, will it be a total or partial exemption?

The other problem with the existing law is that North Dakota credit unions will be at a disadvantage if the present law is maintained. The existing law does not apply to securities firms, insurance companies or any credit provider located outside the State of North Dakota, all of whom are presently offering credit to farmers, businesses, and consumers in North Dakota.

Of concern to credit unions, especially the small credit unions, is the use of third party vendors. Over seventy percent (70%) of the credit unions – the smaller credit unions – outsource their data processing and printing of monthly members' statements including stuffing the envelopes. In addition, all credit unions in North Dakota including five (5) credit unions in South Dakota and one (1) in Minnesota use the VISA credit card services provided by the North Dakota League Service Corp in Bismarck. In order to service their members in a cost effective method, credit unions, especially the smaller credit unions, must be able to outsource services to third parties.

Credit unions have spent thousands of dollars in order to comply with GLB. Regardless of whether this bill passes, The National Credit Union Administration (NCUA) – which insures all credit unions in North Dakota – is requiring North Dakota credit unions to comply with safety and confidentiality of members' records as required by GLB. Attached is a summary of NCUA's Final Rule on guidelines for safeguarding member information. North Dakota credit unions are required by NCUA to comply with GLB in regards to security programs, assessment of potential risks, disclosure of policies and practices, and protecting against unauthorized use of members' personal financial information.

If Senate Bill 2191 does not pass, credit unions will be faced with having to comply with the great majority of GLB requirements because they are federally insured and also attempt to comply with a North Dakota law. The financial burden and difficulty in attempting to meet potentially conflicting federal and state laws will be a nightmare.

Credit unions are in the process of developing privacy notices and disclosures and have spent substantial time and money for that purpose. Credit unions are also facing a time crunch. Notices must be in the mail by June 30, 2001. At this point no one knows what the Federal Trade Commission (FTC) will determine and no one knows when that determination will be made.

The world has changed but the existing law has not.

It is important to all credit unions that all credit granters are on a level playing field with regards to consumer credit information. SB2191 will result in a level playing field – existing law does not. Does North Dakota desire to become an island of nonconformity to the detriment of its business and economic development environment? I hope not!

For credit unions to compete effectively in the market place and to provide for uniform disclosure of information, the North Dakota Credit Union League respectfully requests that the committee send this bill to the House floor with a "Do-Pass" recommendation.

**CUNA REGULATORY ADVOCACY**



**CUNA ANALYSIS- FINAL RULE**

**CREDIT UNION NATIONAL ASSOCIATION**  
805 15<sup>th</sup> Street, NW, Ste. 300  
Washington, DC 20005  
202/682-4200  
FAX: 202/371-8240

**DATE:** January 23, 2001  
**FROM:** Mary Dunn ([mdunn@cuna.com](mailto:mdunn@cuna.com)), Associate General Counsel  
Jeffrey Bloch ([jbloch@cuna.com](mailto:jbloch@cuna.com)), Assistant General Counsel  
**RE:** NCUA's Final Rule on Guidelines for Safeguarding Member Information MAJOR RULE  
**EFF:** July 1, 2001

**EXECUTIVE SUMMARY**

- The final rule amends the National Credit Union Administration's (NCUA's) existing rules regarding security programs in federally-insured credit unions. These amendments are required under the privacy provisions of the Gramm-Leach-Bliley Act (Act).
- The rule requires that a credit union's security program include features to ensure the safety and confidentiality of member's records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to a member.
- Under the privacy rules approved by the NCUA Board on May 8, 2000, credit unions must disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual privacy notices that are sent to members.
- The rule includes an appendix containing Guidelines for safeguarding member information.

If you need a copy of the final rule you may access it on the Internet at the following address:

[http://www.ncua.gov/news/proposed\\_regs/12CFRPart748.pdf](http://www.ncua.gov/news/proposed_regs/12CFRPart748.pdf)

## **BACKGROUND**

The privacy provisions of the Act require the NCUA and other financial institution regulators to establish appropriate standards relating to the administrative, technical, and physical safeguards for consumer records and information. The Act requires that the standards accomplish the following:

- Ensure the security and confidentiality of consumer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records that would result in substantial harm or inconvenience to any consumer.

On May 8, 2000, the NCUA Board approved the final privacy rules that are required under the Act. The rules are effective as of November 13, 2000, although compliance is optional until July 1, 2001. Under these rules, credit unions must disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual privacy notices that are sent to members.

## **DESCRIPTION OF THE FINAL RULE AND GUIDELINES**

### Description of the Final Rule

To fulfill the requirements under the Act, the final rule amends NCUA's existing rules regarding the security programs in federally-insured credit unions. The rule requires that a credit union's security program include features to ensure the safety and confidentiality of member's records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to a member.

The NCUA Board may take administrative action if a credit union fails to establish an adequate security program. This may include cease and desist orders or civil money penalties.

The final rule will be effective on July 1, 2001. Newly-chartered or insured credit unions will need to establish its security program within 90 days from the date of insurance.

### Description of the Guidelines

The Guidelines clarify that "member" has the same meaning as defined in the privacy rules approved on May 8, 2000. As under the privacy rules, "member" includes certain

nonmembers, such as nonmember joint account holders, nonmembers establishing an account at a low-income designated credit union, and nonmembers holding an account in a state-chartered credit union under state law.

Under the Guidelines, the security program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities.

The credit union's board of directors will be responsible for approving the information security program and overseeing efforts to develop, implement, and maintain an effective program. However, the responsibility may be delegated to an appropriate committee of the board. This ability to delegate was suggested in CUNA's comment letter in response to NCUA's proposed rule and Guidelines. The final Guidelines also clarify that specific, day-to-day monitoring is a task that can and should be assigned to management.

To assess risk to member information, credit unions should:

- identify foreseeable internal and external threats that could result in unauthorized use, alteration, or destruction of member information or information systems;
- assess the potential damage of these threats, considering the sensitivity of the member information; and
- assess the sufficiency of policies, procedures, information systems, and other arrangements in place to control risks.

To manage and control risk, each credit union should:

- Design the information security program to control risk, after considering the sensitivity of the information, as well as the complexity and scope of the credit union's activities. The credit unions must consider the following security measures and adopt the ones that are appropriate:
  - Access controls on member information, including controls to prevent pretext calling, which is when unauthorized individuals seek to obtain information by fraudulent means;
  - Access restrictions at physical locations that contain member information;
  - Encryption of electronic information;
  - Procedures designed to ensure that information system modifications are consistent with the credit union's information security program;
  - Dual controls procedures, segregation of duties, and background checks for employees who have responsibilities for, or have access to, member information;
  - Monitoring procedures to detect actual and attempted attacks on information systems;
  - Response programs that specify actions to be taken when the credit union suspects or detects unauthorized access to information systems, including reports to regulatory and law enforcement agencies; and
  - Measures to protect against loss of member information due to potential environmental hazards.

- Train staff to implement the information security program.
- Regularly test the information security program. The frequency and nature of the tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff that is independent of those who develop or maintain the security programs.

With regard to overseeing outsourcing arrangements with service providers, each credit union should:

- Exercise due diligence in selecting service providers.
- Require service providers by contract to implement appropriate measures designed to meet the objectives of the Guidelines.
- If indicated by the credit union's risk assessment, monitor the service providers to confirm that they have implemented the appropriate measures. As part of this monitoring, the credit union should review audits, summaries of test results, or other equivalent evaluations. On-site inspections will not be necessary.

The Guidelines include a two-year grandfather clause with regard to agreements with service providers. This means that until July 1, 2003, contracts that a credit union enters into with a service provider will be acceptable even if the contract does not specifically require the service provider to maintain the security of member information. However, such contracts must be entered into within thirty days after the final rule and Guidelines are published in the *Federal Register*.

With regard to subservicers, credit unions will not have the same level of responsibility, although each credit union must determine that the servicer has adequate controls to ensure that the subservicer will protect member information, consistent with the objectives of these Guidelines.

The Guidelines also include the following standards:

- Each credit union should adjust its information security programs in light of relevant changes in technology, the sensitivity of member information, internal or external threats to the information, and the credit union's own changing business relationships.
- Each credit union should provide an annual report to the board or the appropriate committee of the board. This report should describe the overall status of the information security program and the credit union's compliance with these Guidelines.

TESTIMONY FOR SENATE BILL NO. 2191

House Industry, Business, and Labor Committee

Testimony of Gary D. Preszler, Commissioner, Department of Banking and Financial Institutions neither in support of nor in opposition to Senate Bill No. 2191.

My appearance before this Committee is to provide information to assist the Committee in making an informed decision as to the relationship of North Dakota law with the provisions of the Gramm-Leach-Bliley Bank Modernization Act of 1999 (GLBA). My testimony is not taking a position on the issue of whether opt-in or opt-out is the appropriate public policy view.

*NORTH DAKOTA PRESENT LAW*

The North Dakota Disclosure of Customer Information law (Chapter 6-08.1) was enacted by the 1985 Legislative Assembly after a request by the North Dakota Bankers Association for its introduction.

The North Dakota Disclosure of Customer Information law provides that a "financial institution" has a duty of confidentiality and cannot disclose any customer information to any person, governmental agency, or law enforcement agency unless affirmative consent is granted (opt-in) by the customer, or unless information is obtained through a valid legal process or specifically carved out

under one of the exemptions. North Dakota's law applies to all customers and all information the financial institution has in its possession.

### *GRAMM-LEACH-BLILEY ACT*

The GLBA governs financial institutions' disclosure of non-public consumer information to a non-affiliated third party. Under the GLBA "consumer" is defined as, "an individual who obtains... goods or services, which are to be used primarily for personal, family, or household purposes".

The GLBA does not apply to:

- \* Commercial accounts
- \* Agricultural accounts
- \* Public information.

Section 507(a) of the GLBA provides that a state's financial privacy law is preempted and then only to the extent that the states law or rules are "inconsistent" with the GLBA. Section 507(b) provides that a state law is "not inconsistent" and thus not preempted if it provides "protection ... greater than GLBA's privacy provisions under the Act as determined by the Federal Trade Commission after consultation with the federal functional regulator or 'other authority'".

### *FEDERAL TRADE COMMISSION PETITION*

On September 12, 2000, I petitioned the Federal Trade Commission for a determination under the GLBA as to whether North Dakota's disclosure of customer information statute affords any person greater protection than is provided under GLBA. See attached September 12, 2000, petition. The petition was

requested for several reasons. First, several trade associations had informed me that they preferred the present state law. Second, North Dakota financial institutions need to know the rules of the road.

My petition asks the FTC for a determination that North Dakota law is not inconsistent with the federal law in two areas. First, whether North Dakota's affirmative consent (opt-in) requirement affords greater customer protection than opt-out. Second North Dakota law provides for a civil penalty for violations of Chapter 6-08.1, unlike GLBA that does not provide for any penalty.

I have discussed the petition on a number of occasions with an FTC attorney. Based on these discussions, it is anticipated that the FTC will determine North Dakota's affirmative consent and civil penalties afford greater protection and thus is not inconsistent with the Act.

*SENATE BILL NO. 2191*

The effect of SB 2191 is to eliminate North Dakota's affirmative consent (opt-in) by defaulting to the federal opt-out provisions.

**Further, the Senate amended SB 2191 to remove any state protection for non-public, commercial, or agricultural accounts.**

**Consequently, commercial or agricultural accountholders will not even have the opportunity to opt-out as they will not have any protection under Federal or State law. Financial institutions do not even have to disclose if they**

intend to release information on these accounts to anyone. All information collected on commercial and agriculture accounts, including account numbers, are outside the scope of GLBA.

#### *REGULATORY POSITION*

Although my testimony is given neutral as to the position of opt-in or opt-out, my position as a regulator for state banks and credit unions is to discourage financial institutions from releasing or selling customer information to a third party. Releasing information without proper safeguards creates a potential liability against the bank and consequently may compromise safety and soundness. This is a similar position taken by the Comptroller of the Currency, the regulator for national banks. A recent class action lawsuit proposed settlement against US Bancorp North Dakota bank affiliates point out the validity of this position. US Bank agreed to a proposed class action settlement after a customer alleged the bank, without her consent, violated Chapter 6-08.1 by releasing customer information to a telemarketer that was soliciting credit insurance for a non-affiliated underwriter.

Thank you.

*Testimony in Support of S.B. 2191*  
*Joel Gilbertson*  
*Independent Community Banks of North Dakota*

Mr. Chairman and members of the House Industry, Business and Labor Committee, I am Joel Gilbertson, Executive Vice President and General Counsel of the Independent Community Banks of North Dakota. ICBND is a statewide association of 95 banks located in communities of all sizes throughout our great state.

Community banks have historically been very strong guardians of their customer's privacy and have had a long-standing commitment to protect the confidentiality of customer information. They have jealously guarded the privacy of their customers all over North Dakota.

The entire regulatory environment has changed dramatically with passage of the Gramm-Leach-Bliley Act of 1999. I will not shake the globe again -- but that was the result of GLB. This has been called the most significant change in banking since the 1930's. It has significantly reduced (some would say demolished) the historical firewalls between banking, insurance and securities.

In addition, a very important part of Gramm Leach Bliley was the first venture of the federal government into the complex and controversial area of financial services privacy. It set up a series of privacy requirements that, regardless of whether one might think they are too stringent or not stringent enough, are relatively uniform with respect to requirements for insurance companies, securities firms, credit unions and banks all over the country.

Our present law does not recognize the changes in the financial services industry recognized by Gramm Leach Bliley and that is what SB 2191 is meant to do.

This gets us to the ICBND absolute top priority in this increasingly competitive financial service era. Our community banks strongly believe that the laws and the regulations should be the same for all participants in that arena -- whether they are banks, credit unions, insurance companies or

securities firms. It is for that reason we support SB 2191. It is for that reason as well that we have supported SB 2127, which was heard by this committee last week.

This bill seeks to make the privacy rules the same for all participants in the financial services industry, just as Gramm Leach Bliley has done. It seeks to level the competitive playing field for the insurance, securities and banking sectors. It also allows all of those sectors to be able to rely on meeting the requirements of federal law. It assures banks that if they meet the federal regulations, they will meet all of the privacy requirements necessary.

The present status of this amalgamation of state and federal laws and statutes and their effect on North Dakota banks is confusing and expensive. One smalltown banker told me that to get ready for the July 1 deadline he has ordered notice forms and other forms at a cost of over \$2,000 to comply with GLB requirements. If SB 2191 fails to pass, he said, he will go back to the drawing board and spend another \$2,000 to \$3,000, after trying to determine which parts of state law and which parts of federal law will govern. The irony of all of this, of course, is that at this time this banker does not share any nonpersonal financial information with anyone.

We would like the same consistent standard as everyone else. We want to let our community banks read all of the regulations sent out after Gramm Leach Bliley and know that if they meet those requirements they are ok. We ask for your "Do Pass" recommendation to the North Dakota House. Thank you.



"Preszler, Gary D."  
<gpreszle@state.nd.us>  
s>

To: "Kasper, Jim M." <jkasper@state.nd.us>  
cc:  
Subject: SB 2191 Amendments

03/25/01 10:21 PM

You asked for my comments on proposed amendments 18273.0202 to SB 2191.

The proposed amendments raise a number of questions.

"A financial institution shall notify..... of the financial institution's privacy policies and practices..." **How is the institution to notify the customer and what is to be included in the policies?**

"...[t]he financial institution shall annually allow agricultural and commercial customers to not agree to disclosing that information". **What does this mean and how do customers "not agree"- written, by telephone, e-mail, or other communication?**

Under Section 504 of GLB the federal agencies were required to adopt rules necessary to carry out the purposes of the privacy subtitle. The rules answered these types of questions and provide other guidance for financial entities to comply with GLB. However the federal agencies rules only apply to consumers and not agricultural or commercial accounts.

Further, FTC Chairman Pitofsky recently spoke and reported that there are 12 privacy bills introduced before congress and that he expects that an opt-in will pass this year. If that happens you should be aware that a disparity will exist between consumer, and commercial and agricultural accounts in ND. The proposed amendments then will require North Dakota institutions to provide for an opt-in opportunity for consumers and a "not to agree" (opt-out) opportunity for commercial and agricultural customers.

Gary Preszler, Commissioner  
Department of Banking & Financial Institutions  
2000 Schafer Street, Suite G  
Bismarck, ND 58501-1204  
(701) 328-9933

RL: SB 2191



"Preszler, Gary D."  
<gpreszle@state.nd.us>

To: "Kasper, Jim M." <jkasper@state.nd.us>  
cc:  
Subject: FTC Petition

03/25/01 09:49 PM

Last week you asked about the status of the my petition to the FTC for a determination on the ND affirmative consent privacy law.

I continue to receive weekly calls from an FTC attorney. On last Friday, March 23, 2001, the attorney told me that a new draft letter was sent the previous week to the federal regulatory agencies for comment. I was told that she expected to present the petition to the commission by March 30. She also told me that the recommended decision has not changed and that is that North Dakota's affirmative consent (opt-in) will be determined to afford greater consumer protection than opt-out. According to her since North Dakota is the first petition the final letter needs to be specific on relation to state laws and that is what is taking the time.

If you have any questions, please call.

Gary Preszler, Commissioner  
Department of Banking & Financial Institutions  
2000 Schafer Street, Suite G  
Bismarck, ND 58501-1204  
(701) 328-9933

## NOTICE OF PRIVACY PRACTICES

### UnumProvident Corporation and its subsidiaries

UNUM Life Insurance Company of America  
First UNUM Life Insurance Company  
Provident Life & Accident Insurance Company  
Provident Life & Casualty Insurance Company  
Colonial Life & Accident Insurance Company  
Paul Revere Life Insurance Company  
Paul Revere Protective Life Insurance Company  
Paul Revere Variable Life Insurance Company

Congress recently passed the Gramm-Leach-Bliley (GLB) Act, which deals in part with how financial institutions treat nonpublic personal financial information. UnumProvident Corporation and its insuring subsidiaries have always been committed to maintaining customer confidentiality. We appreciate this opportunity to clarify our privacy practices for you as a result of this new law.

- As part of our insurance business, we obtain certain "nonpublic personal financial information" about you, which for ease of reading we will refer to as "information" in this notice. This information includes information we receive from you on applications or other forms, information about your transactions with us, our affiliates or others, and information we receive from a consumer reporting agency.
- We restrict access to the information to authorized individuals who need to know this information to provide service and products to you.
- We maintain physical, electronic, and procedural safeguards that protect your information.
- We do not disclose this information about you or any former customers to anyone, except as permitted by law.
- Employees share this information outside the company only as authorized by you or for a specific business purpose.
- The law permits us to share this information with our affiliates, including insurance companies and insurance service providers.
- The law also permits us to share this information with companies that perform marketing services for us, or other financial institutions that have joint marketing agreements with us.

We may also share other types of information with our affiliates, including insurance companies and insurance service providers. This information may be financial or other personal information such as employment history and it may not be directly related to our transaction with you. Consistent with the Fair Credit Reporting Act, our standard authorizations permit us to share this information with our affiliates.

**You do not need to call, or do anything as a result of this notice.** It is meant to inform you of how we safeguard your nonpublic personal financial information. You may wish to file this notice with your insurance papers.

If you want to learn more about the GLB Act, please visit our web sites at [www.unum.com](http://www.unum.com) or [www.unum.com/colonial](http://www.unum.com/colonial), or contact your insurance professional.

We value our relationship with you and strive to earn your continued trust.

**Amended Bill Proposed by Representative Kasper  
March 26, 2001**

**FIRST ENGROSSMENT**

Fifty-seventh  
Legislative Assembly  
of North Dakota

**ENGROSSED SENATE BILL NO. 2191**

Introduced by

Senators Krebsbach, Traynor

A BILL for an Act to create and enact 2 new subsections to 6-08.1-01, a new subsection to section 6-08.1-02, a new section to chapter 10-04, a new section to chapter 26.1-02, and a new section to Senate Bill No. 2127 as approved by the fifty-seventh Legislative Assembly of the North Dakota Century Code, relating to disclosure of financial information by financial institutions and the effective date of Section 1 of Senate Bill No. 2127; to amend and reenact section 6-08.1-01 of the North Dakota Century Code, relating to the definitions relating to disclosure of customer information; to provide an effective date, to provide an expiration date, and to declare an emergency.

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

**SECTION 1. AMENDMENT.** Section 6-08.1-01 of the 1999 Supplement to the North Dakota Century Code is amended and reenacted as follows:

**6-08.1-01. Definitions.** As used in this chapter:

1. "Customer" means any person who has transacted or is transacting business with, or has used or is using the services of, a financial institution, or for whom a financial institution has acted as a fiduciary with respect to trust property.
2. "Customer information" means any nonpublic personally identifiable financial information of a customer which is obtained by the financial institution by any means, except for information that is publicly available.

3. "Financial institution" means any organization authorized to do business under state or federal laws relating to financial institutions, including, without limitation, a bank, including the Bank of North Dakota, a savings bank, a trust company, a savings and loan association, or a credit union.

4. "Financial institution regulatory agency" includes:

- a. The federal deposit insurance corporation.
- b. The federal savings and loan insurance corporation.
- c. The national credit union administration.
- d. The federal reserve board.
- e. The United States comptroller of the currency.
- f. The department of banking and financial institutions.
- g. The federal home loan bank board.

5. "Governmental agency" means any agency or department of this state, or any authorized officer, employee, or agent of an agency or department of this state.

6. "Law enforcement agency" means any agency or department of this state or of any political subdivision of this state authorized by law to enforce the law and to conduct or engage in investigations or prosecutions for violations of law.

"SECTION 2. Two new subsections to section 6-08.1-01 of the 1999 Supplement to the North Dakota Century Code are created and enacted as follows:

"Affiliate" means any company that controls, is controlled by, or is under common control with another company.

"Nonaffiliated third party" means any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution. The term does not include a joint employee of such a financial institution."

SECTION 3. A new subsection to section 6-08.1-02 of the 1999 Supplement to the North Dakota Century Code is created and enacted as follows:

A disclosure of customer information by a financial institution to a nonaffiliated third party, if the disclosure is subject to federal law on the date of the disclosure and the financial institution complies with applicable federal law in making the disclosure.

"SECTION 4. A new section to chapter 10-04 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every dealer, agent, investment adviser, federal covered adviser, and investment adviser representative is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section

SECTION 5. A new section to chapter 26 1-02 of the North Dakota Century Code is created and enacted as follows:

Disclosing customer information. Every insurance company, nonprofit health service corporation, and health maintenance organization is a financial institution for purposes of chapter 6-08.1, relating to disclosure of customer information. The commissioner shall enforce compliance with this section.

SECTION 6. A new section to Senate Bill No. 2127, as approved by the fifty-seventh Legislative Assembly, is created and enacted as follows:

SECTION 3. EFFECTIVE DATE. Section 1 of this Act becomes effective on August 1, 2003."

SECTION 7. EFFECTIVE DATE. EXPIRATION DATE: Sections 1, 4, 5, 6, 7 and 8 of this act became effective on July 1, 2001, and Sections 2 and 3 of this act became effective on August 1, 2003. Sections 4 and 5 of this act are effective through July 31, 2003 and after that date are ineffective.

SECTION 8. EMERGENCY. This Act is declared to be an emergency measure.

**CHAPTER 6-08.1  
DISCLOSURE OF CUSTOMER INFORMATION**

**6-08.1-01. Definitions.** As used in this chapter:

*CURRENT LAW - ND*

1. **"Customer"** means any person who has transacted or is transacting business with, or has used or is using the services of, a financial institution, or for whom a financial institution has acted as a fiduciary with respect to trust property.
2. **"Customer information"** means either of the following:
  - a. Any original or any copy of any records held by a financial institution pertaining to a customer's relationship with the financial institution.
  - b. Any information derived from a record described in this subsection.
3. **"Financial institution"** means any organization authorized to do business under state or federal laws relating to financial institutions, including, without limitation, a bank, including the Bank of North Dakota, a savings bank, a trust company, a savings and loan association, or a credit union.
4. **"Financial institution regulatory agency"** means any of the following:
  - a. The federal deposit insurance corporation.
  - b. The federal savings and loan insurance corporation.
  - c. The national credit union administration.
  - d. The federal reserve board.
  - e. The United States comptroller of the currency.
  - f. The department of banking and financial institutions.
  - g. The federal home loan bank board.
5. **"Governmental agency"** means any agency or department of this state, or any authorized officer, employee, or agent of an agency or department of this state.
6. **"Law enforcement agency"** means any agency or department of this state or of any political subdivision of this state authorized by law to enforce the law and to conduct or engage in investigations or prosecutions for violations of law.
7. **"Person"** means any individual, partnership, corporation, limited liability company, association, trust, or other legal entity.

**6-08.1-02. Exemptions.** This chapter does not apply to any of the following:

1. The preparation, examination, handling, or maintenance of any customer information by any officer, employee, or agent of a financial institution having custody of such information or the examination of such information by an accountant engaged by the financial institution to perform an audit.
2. The examination of any customer information by, or the furnishing of customer information to, any officer, employee, or agent of a financial institution regulatory agency solely for use in the exercise of his duties.

3. The publication of data derived from customer information where the data cannot be identified to any particular customer or account.
4. Any acts required of the financial institution by the Internal Revenue Code.
5. Disclosures permitted under the Uniform Commercial Code concerning the dishonor of any negotiable instrument.
6. The exchange in the regular course of business of customer credit information between a financial institution and other financial institutions or commercial entities, directly, or through a customer reporting agency.

7. The release by the Industrial Commission, in its capacity as the managing body of the Bank of North Dakota, of either of the following:

- a. The name of any person who, either directly or indirectly, has obtained financing through the Bank of North Dakota.
- b. The amount of any financing obtained either directly or indirectly through the Bank of North Dakota.

8. An examination, handling, or maintenance of any customer information by any governmental agency or law enforcement agency for purposes of verifying information necessary in the licensing process, provided prior consent is obtained from the licensee and customer.

9. Disclosure of customer information to a law enforcement agency or governmental agency pursuant to a search warrant or subpoena duces tecum issued in accordance with applicable statutes or the North Dakota Rules of Criminal Procedure.

10. Disclosure by a financial institution to the commissioner of agriculture that it has given a customer notice of the availability of the North Dakota agricultural mediation service.

11. The disclosure by a financial institution to any financial institution or other entity that controls, is controlled by, or is under common control with the financial institution if the financial institution or other entity receiving the information complies with section 6-08.1-03.

**6-08.1-03. Duty of confidentiality.** A financial institution may not disclose customer information to any person, governmental agency, or law enforcement agency unless the disclosure is made in accordance with any of the following:

1. Pursuant to consent granted by the customer in accordance with this chapter.
2. To a person other than a governmental agency or law enforcement agency pursuant to valid legal process.
3. To a governmental agency or law enforcement agency pursuant to valid legal process in accordance with this chapter.
4. For the purpose of reporting a suspected violation of the law in accordance with this chapter.
5. For the purpose of notifying the commissioner of agriculture that a financial institution has notified a customer of the availability of the North Dakota agricultural mediation service.

*Mrs. Stearns makes ND Bank public information*

*This has always been public information*

*Affiliate Exemption*

## **Amendments to SB 2191 Adopted by North Dakota House**

The amendments to SB 2191 adopted by the House simply extends the privacy protections of the Gramm-Leach-Bliley federal law to commercial and ag customers. The federal law only applies to consumer customers and financial institutions in the state, under the amendment, will be required to provide their privacy policy and "opt-out" notice, if customer information is shared with third parties, to all commercial and ag customers, in addition to consumer customers. It is believed North Dakota is the only state to expand these privacy protections to commercial and ag customers of financial institutions.

This amendment sunsets in two years in view of the anticipated recommendations resulting from the interim privacy study under SCR 4019.

It is recommended that the Senate concur with the House amendments.

Independent Community Banks of North Dakota  
North Dakota Credit Union League  
North Dakota Bankers Association  
North Dakota Professional Insurance Association  
North Dakota Retail Association  
American Insurance Association

# COVINGTON & BURLING

1201 PENNSYLVANIA AVENUE NW  
WASHINGTON, DC 20004-2401  
TEL 202.682.6000  
FAX 202.682.6281  
WWW.COV.COM

WASHINGTON, DC  
NEW YORK  
LONDON  
BRUSSELS  
SAN FRANCISCO

June 2, 2000

## MEMORANDUM

### Analysis of Final Regulations Implementing the Financial Privacy Provisions of the Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (the "Act"), which was signed by the President and enacted into law on November 12, 1999,<sup>1</sup> substantially changes and reforms the regulation of the financial services industry. Title V of the Act establishes financial privacy protections for retail consumers of financial institutions, and final regulations implementing these protections have now been issued in virtually identical form by financial institution regulatory agencies and the Federal Trade Commission.<sup>2</sup> (The privacy regulations are collectively referred to in this memorandum as "the Rule".) The Rule technically takes effect on November 13, 2000, but covered institutions are not obligated to come into compliance until July 1, 2001.

### 4 REQUIREMENTS OF GLB

The Act subjects financial institutions to four new requirements regarding the nonpublic personal information of their consumers. Each financial institution must:

- (1) *Clearly and conspicuously give notice to each consumer – at least once each year for ongoing customers – of its policies for collecting and sharing the consumer's nonpublic personal information.*

<sup>1</sup> Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); H.R. Conf. Rep. No. 434, 106<sup>th</sup> Cong., 1<sup>st</sup> Sess. (1999).

<sup>2</sup> *Joint Final Rule - Privacy of Consumer Financial Information*, 65 Fed. Reg. 35,161 (2000) (to be codified at 12 C.F.R. Part 40 (Office of the Comptroller of the Currency), 12 C.F.R. Part 216 (Board of Governors of the Federal Reserve System), 12 C.F.R. Part 332 (Federal Deposit Insurance Corporation), 12 C.F.R. Part 573 (Office of Thrift Supervision); *Final Rule - Privacy of Consumer Financial Information*, 65 Fed. Reg. 31,721 (2000) (to be codified at 12 C.F.R. Part 716) (National Credit Union Administration); and *Final Rule - Privacy of Consumer Financial Information*, 65 Fed. Reg. 3645 (2000) (to be codified at 16 C.F.R. Part 313) (Federal Trade Commission). The Securities and Exchange Commission version of the regulation is expected to be issued shortly in substantially the same form as the other regulations. State insurance commissioners, which have authority to issue regulations applicable to the insurance organizations they regulate, have yet to issue proposed or final regulations – although the Act's statutory obligations applicable to such organizations become effective on November 13, 2000.

- (2) Afford consumers choice, i.e., the right to "opt out" of disclosures to non-affiliated third parties, subject to certain exceptions.
  - No opt-out applies with respect to disclosures to affiliates.
- (3) Not disclose account access information of consumers to third party marketers.
- (4) Abide by regulatory standards to protect the security and confidentiality of its consumers' nonpublic personal information.

These four new obligations are subject to enforcement by the financial institution regulators and the Federal Trade Commission, depending on the type of financial institution involved. In addition to the four new obligations imposed on financial institutions, the Act prohibits the practice of "pretext calling" in which someone fraudulently obtains or causes the disclosure of customer information from a financial institution by fraudulent or deceptive means. These and other privacy provisions in the Act are explained in more detail below.

A. Scope of Coverage/Key Definitions

The Act's privacy protections apply to the "nonpublic personal information" of "consumers" and "customers" of "financial institutions." Because the Rule's definitions of these key terms are expansive, the scope of the Act's privacy protections is broad.

1. "Financial Institution"

WHO IS INCLUDED

As defined by the Rule, the term "financial institution" means any institution that is "significantly engaged in financial activities." This definition clearly extends to any kind of traditional, regulated financial company, including banks, bank holding companies, financial holding companies, securities firms, insurance companies, insurance agencies, investment companies, thrifts, and credit unions. But the definition also includes any other type of business that is significantly engaged in financial activities, whether or not the institution is regulated or otherwise considered to be a financial company. Thus, the Act's new privacy restrictions will extend to such institutions as mortgage brokers, finance companies, and check cashers.

In addition, the term "financial activities" means virtually any activity that is permissible for a "financial holding company" (which is a new type of bank holding company created by other parts of the Act) and includes certain types of activities that are not typically considered to be "financial." As a result, the Act's restrictions will also extend to tax preparation firms, financial data processors, and financial software companies.

Moreover, a company that engages primarily in commercial activities, but also engages "significantly" in financial activities, will be deemed to be a covered "financial institution" with respect to the consumers of those financial activities. For example, a retailer that issues its own credit card will be a covered "financial institution" with respect to

its credit card customers, but will not be directly subject to the Act's obligations with respect to its general retail activities.

2. "Consumer" and "Customer"

The Rule defines "consumer" and "customer" differently, and the difference is significant for purposes of the Act's obligations.

A "consumer" of a financial institution means an individual who obtains a financial product or service from the institution primarily for personal, family, or household purposes; it does not include any corporate entity or any individual or corporate business customer. The Rule broadly defines this term to cover individuals who may have only occasional or isolated contacts with a financial institution, such as someone who uses an ATM of a bank where he or she is not a depositor, or someone who merely purchases travelers' checks from an institution. The term also covers someone who merely applies to obtain a financial product or service (such as a loan), even if the person's application is rejected.

A "customer" is a particular type of "consumer," i.e., a consumer who establishes a "continuing relationship" with a financial institution, such as a depositor, borrower, or insurance policyholder.

**DIFFERENCE**

The significance of the distinction between a "consumer" and a "customer" is as follows. A financial institution does not need to provide a privacy notice to a mere "consumer" (one that is not a "customer") unless the institution intends to disclose that individual's nonpublic personal information to nonaffiliated third parties. Even if the financial institution does intend to make such third party disclosures, it may provide a "short form" notice to the consumer, and there is no obligation to provide annual notices to the consumer thereafter.

In contrast, a "customer" must be provided an initial privacy notice at the time the customer relationship is established, whether or not the financial institution plans to disclose the customer's nonpublic personal information to others, and the short-form notice is not permitted. Thereafter, the customer must also be provided annual privacy notices.

3. "Nonpublic Personal Information"

The term "nonpublic personal information" (or "NPI") means any "personally identifiable financial information" of a consumer that is obtained by the financial institution by virtually any means, except for information that is otherwise publicly available. The definition expressly extends to any list, description, or grouping of consumers - including publicly available information about those consumers - that is derived using nonpublic personal information.

Once again, the Rule construes these terms broadly. NPI does not have to be "financial" in the traditional sense of describing someone's account balances or payment

information. It also includes the mere fact that someone has a customer relationship with a financial institution, which would sweep in all customer lists, as well as the mere fact that a consumer has purchased a product from the financial institution. And it includes any information collected through an Internet "cookie."

In addition, the exception for publicly available information, while subject to much debate, appears to be of little practical use. This is so because any truly publicly available information (such as a name or address) that is derived in any way from NPI (e.g., the names and addresses of customers or of people who have certain payment histories) is not subject to the exception - and most disclosures of publicly available customer information are in fact derived from NPI in some way.

*Key* In short, NPI as a practical matter appears to include just about all personally identifiable information that a financial institution has in its possession pertaining to one of its retail consumers.

B. Notice: Initial and Annual Disclosures *Notice to Consumers*

Under the circumstances described below, a financial institution must provide notice of its privacy policies and practices to its consumers.

1. Contents of Notice

The Rule is quite specific about the types of information that must be disclosed in privacy notices, which as a practical matter is likely to include the required "opt out" disclosures that must also be provided to consumers. As described in the next section, the required information need not be exceptionally detailed. Nevertheless, a financial institution's careful analysis of the types of information that must be provided in the initial and annual privacy notices will provide a key starting point for determining the scope of its compliance obligations under the Rule.

There are nine specific categories of information that must be included in both the initial and annual privacy notices (other than the short-form notice):

- (1) **Categories of NPI collected.** Statement as to whether information is collected from the consumer from applications or other forms; from transactions that the consumer has with the financial institution, its affiliates, or others; or from credit bureaus.
- (2) **Categories of NPI disclosed to others.** Brief description of the types of information collected by the financial institution that is or may be disclosed to other entities. This could be all consumer information collected, or it could be a brief description of the types of information collected directly from the consumer (e.g., name, address, income, assets, etc.); the types of information collected from transactions the consumer has with the institution or with others (e.g., payment history,

institution may provide the first annual privacy notice at any time before December 31 of year 2, and once each calendar year thereafter.

4. Other Notice Issues

A holding company may own several different "financial institution" subsidiaries within the same corporate family. These separate subsidiaries may have common customers. In such circumstances, the Rule provides the holding company a choice. It may create a unified privacy notice that applies to all of its subsidiaries, and it may provide a single unified notice to any person who is a consumer of more than one of the subsidiaries. Or it may have different notices for different subsidiaries, which would mean that an individual could receive more than one privacy notice from the same corporate organization.

Most corporate organizations will likely prefer to use a single, unified notice in order to avoid confusing customers and in order to avoid the complexity of using multiple databases for customers that choose to opt out. However, such organizations may not have unified databases that would permit the creation and implementation of a unified privacy notice.

Finally, it is currently estimated that approximately 40,000 entities qualify as "financial institutions" under the Rule, and that approximately 2.5 billion privacy notices will be sent to individuals next year. This large number reflects the fact that individuals typically have relationships with many different "financial institutions," and thus will receive many different privacy notices.

② Choice: Customer "Opt-Out" of Disclosures to Third Parties OPT-OUT

The Act's second basic privacy obligation for financial institutions is the requirement that a consumer be afforded the right to prevent the disclosure of nonpublic personal information to a nonaffiliated third party – commonly referred to as the right to "opt out."

1. General Requirement

A financial institution may not disclose nonpublic personal information to a "nonaffiliated third party" unless—

- ① • The financial institution clearly and conspicuously discloses to the consumer that such information may be disclosed to the third party;
- ② • The consumer is given the opportunity to direct that the information not be disclosed to the third party (the right to "opt out"); and
- ③ • The consumer is given an explanation of how to exercise the opt-out.

The financial institution does *not* have to provide the right to opt out when the information is provided to an *affiliate*, as opposed to a nonaffiliated third party. In addition, "nonaffiliated third party" is defined as an entity that is not under common control with the financial institution, but does not include a "joint employee." As a result, the opt-out need not be provided if the financial institution provides the information to its employee who happens also to be an employee of a nonaffiliated third party.

2. General Exceptions to Notice - OPT-OUT

There are a number of significant exceptions that permit a financial institution to disclose NPI to third parties regardless of the consumer's opt-out preference. These general exceptions are intended to address situations, among others, where the disclosure is: necessary to process a transaction requested or authorized by the customer (e.g., making a payment); necessary to effect, administer, or enforce a transaction; made with the specific consent of the consumer; made to protect against fraud; made to a consumer reporting agency; made in connection with a merger or sale of the financial institution; made to comply with a regulatory investigation; made to lawyers and auditors; and other circumstances where an opt out would not be practical or expected to be provided.

3. Service Provider/Joint Marketing Exception PROTECTION FOR SERVICES

In addition to the general exceptions, an exception to the opt-out requirement applies where a financial institution discloses information to a nonaffiliated third party to perform services on behalf of the financial institution. Such services of the third party may include marketing of the financial institution's own products. In addition, the exception covers disclosures to third parties pursuant to joint marketing arrangements with other financial institutions (under which the two financial institutions jointly offer, endorse, or sponsor a financial product or service).

The service provider/joint marketing exception is different from the general exceptions in two ways. First, disclosures made under the service provider exception are subject to a special notice requirement: one of the nine mandatory items in the privacy notice requires (a) a description of the categories of NPI disclosed under this exception; and (b) a statement as to whether the third party receiving the information performs marketing services for the financial institution, or is another financial institution with whom the first financial institution has a joint marketing agreement. Second, a financial institution may not take advantage of the service provider/joint marketing exception unless it enters into a contract with the third party that generally prohibits the entity from disclosing or using the NPI it receives other than to carry out the purposes for which the information was disclosed.

4. Form and Timing of Opt-Out Notice

A financial institution's disclosure of the consumer's right to opt out -- the opt-out notice -- may be included as part of the initial and annual privacy notice, and it is anticipated that most institutions will do so. That is, as described above, one of the nine mandatory items in the privacy notice is a description of the consumer's right to opt out, and

not otherwise regulated as a "financial institution," as well as over any nonfinancial institution recipient of NPI from a financial institution under the re-disclosure and re-use restrictions.) As noted previously, these regulators have issued virtually identical versions of the Rule to implement the new statutory provisions. Each regulatory agency may enforce both the statute and Rule with respect to financial institutions under their respective jurisdictions using the general enforcement powers granted to them under their enabling statutes. The Act did not, however, create a private right of action for consumers as a remedy for violations of the Act or the Rule.

G. Relation Between Federal and State Laws

"States Can Pre-empt OPT-IN"

The Act generally provides that the new federal privacy provisions will preempt only those state laws that are inconsistent with the new federal laws. But such preemption will not apply if the state law provides greater privacy protection than the federal law, as determined by the FTC. However, this preemption provision and its exception apply only to the Act's privacy provisions. Nothing in the privacy provisions of Title V of the Act affects federal preemption provisions in other statutes, including the preemption provisions of the FCRA. As a result, notwithstanding arguments to the contrary, the FCRA's preemption of state restrictions on information sharing among affiliated companies remains intact with respect to any state law passed before January 1, 2004 (including new state law "opt in" restrictions).

H. Effective Date

As mentioned previously, the effective date of the Rule is technically November 13, 2000, but financial institutions are not required to be in compliance until July 1, 2001. This later date is a bit misleading, however, at least for those institutions that will want to share NPI with nonaffiliated third parties as of that date with respect to customers who have not opted out. In order to share a customer's NPI as of that date, a financial institution will have had to have sent opt-out notices to customers at least 30 days before the July 1 deadline in order to provide customers with a reasonable opportunity to opt out, as required by the Rule.

In addition, the financial institution must have a system in place that allows it to comply with a consumer's opt out direction "as soon as reasonably practicable" after the financial institution receives it. The estimated amount of time it takes to enter a consumer's opt-out choice into its compliance system must be tacked on to the 30-day period in order for financial institutions to have a credible database that reflects consumer opt-out preferences as of July 1, 2001. That additional time could prove to be substantial in the initial stages of compliance with the privacy Rule. If so, a financial institution could be forced to begin sending the privacy/opt-out notices to customers by April or May of 2001 in order to be in a position to share (or continue to share) NPI with nonaffiliated third parties as of the July 1, 2001 effective date.

fall within the opt-out notice requirement, and a clarification that the term "nonpublic personal information" does not encompass lists or descriptions derived without using any nonpublic personal information.

Smaller financial institutions fought hard in Conference for the expansion of the notice and opt-out requirements to include affiliates of financial institutions as well as third parties, arguing that permitting information to be freely shared among affiliates places them at a competitive disadvantage. Although they were supported in this effort by consumer groups, privacy advocacy groups and initially, the Administration, the compromise ultimately did not expand upon the structure agreed to in the House. The result of their effort is hortatory language in the Conference Report urging that "agencies and authorities described in section 504(a)(1) should take into consideration any adverse competitive effects on small commercial banks, thrifts and credit unions."

As an accommodation to certain software manufacturers, the GLB Act also includes hortatory language allowing that agencies and Departments may permit by regulation disclosures in an "encrypted, scrambled, or similarly coded form".

**B. Overview**

## OVERVIEW OF GLB

The Title V privacy provisions of the GLB Act now include the following:

1. • A new "affirmative and continuing" obligation to safeguard privacy applicable to all firms that engage in financial services (not just banks or traditional finance service providers), as well as to firms engaged in activities "incidental" to financial activities.
2. • A requirement that each financial regulator establish "standards" to implement this privacy obligation.
3. • A general privacy disclosure to consumers about the institution's privacy policy, including its policies concerning information sharing with affiliates and third parties, which is required upon opening an account or beginning a relationship and reiterated not less than annually. A separate opt-out disclaimer with respect to the transfer of information to unaffiliated third parties also upon the opening of an account [or beginning of a relationship] and not less than annually thereafter.
4. • A prohibition against transfers of "nonpublic personal information" to unaffiliated third parties, unless the possibility of such transfers and the option to opt-out are disclosed and the customer has been given the opportunity to "opt-out".
5. • Numerous specific exceptions that permit disclosures to third parties without providing notice or opportunity to opt-out.
6. • A mandate that the bank regulators, the NCUA, the Treasury and the SEC, in consultation with the FTC and representatives of state insurance regulators,

engage in separate "coordinated" rule-makings to detail how the two disclosures should be provided and what they should include.

- 7. • A requirement that the Treasury Department study information sharing practices among financial institutions and their affiliates.
- 8. • A prohibition against the practice of "pretext calling" that includes criminal sanctions.

**C. Duty to Protect Consumer Information**  
*Sec. 501 (pp. 99-100)*

The privacy provisions of the GLB Act impose on each "financial institution" an "affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information." Section 501(a). To accomplish this goal, the GLB Act requires each functional regulator to issue "appropriate standards for the financial institutions subject to their jurisdiction" to insure "the security and confidentiality of customer records and information;" to protect against "any anticipated threats or hazards to the security or integrity of such records;" and "to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

This is a broad mandate that each functional regulator will have to interpret, and the Act provides no means for ensuring consistent interpretations. Moreover, it is not clear whether the term "standards" necessarily requires rulemaking. It is quite possible that a regulator could issue a loose directive to protect the security and confidentiality of customer records, while another could issue detailed regulations covering a wide range of activity.

The term "consumer" is defined as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."

CONSUMER

**D. Opt-Out for Third-Party Sharing**  
*Sec. 502 (pp. 100-102); Sec. 509(5) (p. 107-108)*

OPT-OUT

As noted above, the most publicized and controversial part of the privacy provisions of the GLB Act is its requirement that financial institutions may not disclose "nonpublic personal information" to nonaffiliated third parties unless they provide a specific opt-out notice to consumers and the opportunity to opt-out prior to such third party sharing. The Act provides that such notice must be provided "clearly and conspicuously," in "writing or in electronic form, or other form permitted by regulation." The notice must provide consumers with an explanation of how to direct that their information not be disclosed, and an opportunity to exercise this option prior to disclosure to an affiliated third party.

"Nonaffiliated third party" is defined to mean any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution.

NON Affiliates

1. **General Exception for Marketing and Servicing**  
Sec. 502(b)(2) (p. 100)

The GLB Act provides a general exception for providing nonpublic personal information to third parties to perform services or functions on behalf of the financial institution intended to cover transfers necessary for joint marketing arrangements, or to facilitate a third party servicing of consumer accounts. However, these transfers must be fully disclosed to consumers, and financial institutions must enter into contractual agreements with the third parties that require the third parties to "maintain the confidentiality of such information."

2. **Specific Exceptions**  
Sec. 502(e) (p. 101), Sec. 509(7) (p. 107)

Affiliates

The GLB Act further provides a number of specific exceptions for circumstances that do not require that any notice be given to consumers prior to disclosure of nonpublic personal data to some third parties. However, if any third party disclosure does not fall completely within one or more of these exceptions, then the notice and opportunity to opt-out must be provided. These include the following circumstances: **NO NOTICE REQUIRED**

- 1. Transfers "as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer" in connection with servicing or processing a financial product or service, maintaining or servicing the consumer's account, or a proposed or actual securitization, secondary market sale or similar transaction. ("As necessary to effect, administer, or enforce the transaction" is defined in detail in Section 509(7).)
- 2. Transfers made with the consent or at the direction of the consumer.
- 3. Transfers made to protect the confidentiality or security of a consumer's records, to protect against fraud, unauthorized transactions, for required institutional risk control or other liability, or for resolving customer disputes or inquiries.
- 4. Transfers to persons holding a beneficial interest relating to the consumer, or to persons acting in a fiduciary or representative capacity on behalf of the consumer.
- 5. Transfers to provide information to an insurance rate advisory organization, guaranty fund or agency, a credit rating agency, and to permit the assessment of the financial institution's compliance with industry standards.
- 6. Transfers to the financial institution's attorneys, accountants and auditors.
- 7. Transfers permitted or required under other laws and in accordance with the Right to Financial Privacy Act of 1978, to law enforcement agencies (including federal functional regulators; the secretary of the Treasury with respect to the Bank Secrecy Act, state insurance authorities or the Federal Trade Commission), self-

regulatory organizations, or for an investigation on a matter related to public safety.

- 8. Transfers to a consumer reporting agency, and transfers from a consumer report produced by a consumer reporting agency in compliance with the Fair Credit Reporting Act, in accordance with interpretations of such Act by the Board of Governors of the Federal Reserve System or the Federal Trade Commission.
- 9. Transfers in connection with a sale, merger, transfer, or exchange of all or a portion of the business or operating unit of the financial institution if the disclosure concerns only customers of that business or unit.
- 10. To comply with federal, state, or local laws, rules, and to comply with civil, criminal, or regulatory investigations, federal, state or local summons or subpoenas or to respond to judicial process of government authorities with jurisdiction over the financial institution under these authorities.

**3. Limits on Reuse of Information**  
*Sec. 502(c) (p. 100)*

Unaffiliated third parties that receive nonpublic personal information from a financial institution for *any* purpose (including pursuant to the exceptions set forth above) may only disclose such information if "such disclosure would be lawful if made directly to such other person by the financial institution." This effectively makes third parties that receive nonpublic personal information from financial institutions subject to the these provisions of the law.

**4. Prohibition on Sale of Account Information for Telemarketing**  
*Sec. 502(d) (pp. 100-101)*

The GLB Act includes a provision to address the kinds of abuses involving the sale of customer account information to third party telemarketers that have recently received so much publicity. Disclosures of account numbers or similar access numbers or credit card numbers or access codes information to third parties for use in telemarketing, direct mail marketing or other marketing through electronic mail is expressly prohibited.

**E. Disclosure of Privacy Policy and Procedure**  
*Sec. 503 (p. 102)*

Each financial institution is required by the GLB Act to make certain required disclosures of its privacy policies to each consumer, both at the time of establishing a customer relationship and then "not less than annually" during the continuation of the relationship. These disclosures, which must be clear and conspicuous, may be made either in writing or in electronic form or other form authorized by regulation, must set forth the institution's privacy policies and practices and must include:

Act to clarify that the federal banking agencies have the authority to issue regulations "as necessary" to detect and enforce privacy violations that may occur during the transfer of, and process of correcting information given by banks to reporting agencies.

H. Relation to State Privacy Laws  
*Sec. 507 (p. 105)*

"States Can Protect  
Privacy"

The GLB Act provides that the privacy provisions of the Act shall not preempt, alter or affect any state law or regulation, except to the extent such laws or regulations are inconsistent with the provisions of the Act and then only to the extent of the inconsistency.

Section 507 (b) further explicitly states that state law will not be considered to be inconsistent with federal law for these purposes if the protection such state -

"statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subtitle... as determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction under section 505(a) of... either the person that initiated the complaint or that is the subject of the complaint, on its own motion or upon the petition of any interested party."

ND  
CURRENT  
LAW!  
OPT-IN

This provision was adopted in Conference with the support of consumer groups and privacy advocates. It may effectively undermine the force of Title V as a national standard, and cause the privacy debate to resume in various state capitals. This was the stated intention of its supporters, and state attorney generals may examine ways to correct what they perceive as the inadequacies of the federal law.

However, an obscure provision of the Fair Credit Reporting Act ("FCR Act") could prove to be an obstacle to state action on the privacy issue with respect to information sharing among affiliated institutions. Section 1681 of the FCR Act states "no requirement or prohibition may be imposed under the laws of any State with respect to the exchange of information among persons affiliated by common ownership or common corporate control." It is not clear whether this provision, which has not been tested in court, will impede efforts by the states to legislate in this area.

I. Study of Information Sharing Among Financial Affiliates  
*Sec. 508 (pp. 105-106)*

In lieu of any restrictions on information sharing among affiliates of FHCs, the GLB Act directs the Treasury, in conjunction with the federal functional financial regulatory agencies and the FTC, to conduct a comprehensive study of current information sharing practices among financial institutions and their affiliates and unaffiliated third parties, and to report to Congress with its findings and recommendations for legislative or administrative action by January 1, 2002. In conducting this study, the Treasury is directed to consult with representatives of the state insurance authorities, etc. However, in his statement at the signing of the bill, President Clinton announced that he was directing the National Economic Council to work with Treasury and Office of Management and Budget to complete the study and recommendations next year.

**J. Definitions**

*Sec. 509 (pp. 106-108)*

**1. "Financial Institution"**

The definitions make clear that these provisions are intended to be applied to all institutions participating in the delivery of financial services to customers. The term "financial institution" is defined to be "any institution the business of which is engaging in financial activities as described in new Section 4(k) of the Bank Holding Company Act of 1956." Specifically excluded from the definition of "financial institution" are persons or entities subject to the jurisdiction of the CFTC, the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971.

**2. "Consumer"**

It defines a "consumer" as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." The definition makes explicit that Section 502 and 503 privacy notice provisions apply only to retail transactions with individuals, and do not apply to corporate or business data or business customers.

Key

**K. Pretext Calling**

*Sec. 521-527 (pp. 109-113)*

Subtitle B of Title V incorporates the provisions protecting consumers from the "identity fraud" that had been added to the Senate bill by Senator Sarbanes. The Act provides civil and criminal penalties for those who obtain personal information by fraud or deception from either an individual or a financial institution. The Act also grants new enforcement authority to the FTC.

The Act specifically prohibits any person from obtaining or attempting to obtain customer information relating to another person by making a "false, fictitious, or fraudulent statement or representation" to an employee or agent of a financial institution, a customer of an institution, or through the use of a forged or false document to such an institution. Moreover, requesting another person to obtain personal financial information in a manner that violates this section is also a violation under the Act. The Act excepts law enforcement agencies and insurance institutions investigating insurance fraud from the reach of these provisions, and provides exceptions for financial institutions in certain circumstances including testing security procedures, investigating allegations of misconduct on the part of an employee and recovering customer information of the institution which was obtained or received by another person.

The Act provides that the identity fraud provisions will be enforced by the FTC "in the same manner and with the same power and authority as the Commission has under the Fair Debt Collection Practices Act." Sec. 522(a) The federal banking regulators are also authorized to enforce compliance by institutions under their respective jurisdictions.