

1 **TITLE:** **FINANCIAL INFORMATIONS SECURITY**

2
3 **COMMITTEE:** **NCSL STANDING COMMITTEE ON COMMUNICATIONS,**
4 **FINANCIAL SERVICES & INTERSTATE COMMERCE**

5
6 **TYPE:** **DRAFT - POLICY STATEMENT**

7
8 Americans place great value on the right to privacy, and general support for privacy and
9 confidentiality protections has increased as the ability of individuals to seclude personal
10 matters from the sight, presence and intrusion of others has diminished. In the
11 *Information Age*—where vast quantities of information drive economic activity—familiar
12 and unfamiliar entities continuously gather, solicit, manage and share personally
13 identifiable data, which commonly includes financial records, medical histories, and
14 information on routine consumer transactions. Although much of this information has
15 long been available in pieces, its conversion into electronic form and concentration into
16 massive, centralized information systems has significantly eroded an individual’s ability
17 to condition or control his or her personal information. It also threatens the
18 confidentiality of information by heightening the likelihood that data—if not one’s
19 identity—will be improperly disclosed, stolen or misused with potentially significant
20 economic harm to the individual.

21
22 Protecting personal information traditionally has been a state responsibility. All states
23 have laws to safeguard the security of financial information, and state legislatures
24 continue to consider and enact legislation annually to improve and strengthen financial
25 information security. Congress also has enacted laws to protect financial privacy and
26 confidentiality and to ensure the accuracy of financial information. Federal interest and
27 activity in this area has increased with the onset of the Information Age.

28

29 **Fair Credit Reporting Act (FCRA)**

30 Personal financial information was protected exclusively at the state level until 1970
31 when Congress enacted the Fair Credit Reporting Act (FCRA). FCRA established
32 minimum federal standards to ensure that consumers could access information about
33 themselves that lenders, insurers, and others obtain from credit bureaus and use to
34 make decisions about providing credit and other services. Amendments to FCRA,
35 enacted in 1996, imposed new responsibilities on credit bureaus and those who use
36 their information to promote increased accuracy and confidentiality of credit reports. The
37 1996 Amendments also temporarily preempted, with a limited number of grandfathered
38 exceptions, stronger state laws in seven areas. These included prescreening of
39 consumer reports; the timeframe for handling accuracy disputes; duties of persons who
40 take adverse actions and who use consumer reports in connection with credit or
41 insurance transactions initiated by a consumer; information contained in consumer
42 reports; duties of furnishers of information to consumer reporting agencies; and the
43 sharing of information among affiliates.

44

45 Congress reauthorized and made permanent the seven areas of state preemption prior
46 to their expiration with the Fair and Accurate Credit Transactions (FACT) Act of 2003
47 while further enhancing the accuracy of credit reports, providing consumers one free
48 credit report annually, restricting the use of sensitive information from affiliates to market
49 financial products, and establishing several uniform consumer protections to combat
50 identity theft. Although virtually all the federal anti-identity theft protections in the FACT

51 Act were based on state laws, the measure also preempts state laws in each of the
52 areas where it established federal protection.

53

54 **Gramm-Leach-Bliley**

55 In addition to FCRA, Congress passed significant financial privacy protections with the
56 Gramm-Leach-Bliley Financial Modernization Act (GLBA) of 1999 that applied to a wide
57 range of financial institutions. GLBA required financial institutions to provide notice to its
58 customers on its privacy policies, including how information is disclosed to affiliates and
59 nonaffiliated third parties, and to offer consumers the opportunity to “opt out” of having
60 nonpublic personal information shared with nonaffiliated third parties. Although FCRA
61 continues to preempt state laws that would restrict information sharing among affiliates,
62 GLBA expressly permits states to exceed the federal standards for nonaffiliated third
63 parties. GLBA also required states to establish minimum privacy protections for the
64 insurance consumers—a requirement that states promptly met.

65

66 **Financial Information Security**

67 The National Conference of State Legislatures (NCSL) believes that states should
68 continue to play a vital role in protecting the privacy, confidentiality and security of
69 sensitive nonpublic personal financial information. States long have sought to balance
70 the economic value of information sharing with reasonable safeguards against the
71 unnecessary disclosure and inappropriate acquisition of sensitive nonpublic personal
72 financial information, such as credit information, account numbers, account balances,
73 and Social Security numbers. Understanding local and regional economic situations and

74 the unique needs of consumers within these markets, states consistently have ensured
75 the protection of sensitive non-public personal financial information.

76

77 State legislatures recognize that financial information security is an area of overlapping
78 federal and state jurisdiction. Therefore, NCSL does not oppose federal baseline
79 standards for the protection of financial information, provided that these standards
80 generally do not preempt complementary state laws. NCSL believes that states should
81 have the authority and flexibility to adopt standards for the acquisition, retention,
82 disclosure and sharing of financial information by and among financial institutions and
83 nonaffiliated third parties that address local concerns or respond in a timely way to
84 incidences of neglect or abuse that may be local or regional in nature. NCSL specifically
85 believes that Congress should preserve state authority to exceed federal baseline
86 standards for information sharing among nonaffiliated third parties.

87

88 **Credit Reporting**

89 NCSL acknowledges the benefit of a uniform national credit reporting system to the
90 nation's economy. Therefore, NCSL does not oppose the seven limited areas that were
91 subject to federal preemption by the 1996 Amendments of the FCRA and made
92 permanent by the FACT Act. In doing so, NCSL supports the continued exemption of
93 the state laws that were in existence prior to the 1996 Amendments and thus are
94 currently exempted from the preemption provisions.

95

96 **Data Security Breach Disclosure**

97 Following a series of high-profile financial data security breaches, Congress is
98 considering a range of measures to establish additional federal protections for financial
99 data and to guard against identity theft and account fraud. Federal interest comes on
100 the heels of laws passed in many states that require institutions to notify affected
101 consumers following a data security breach. In fact, many of the reported breaches only
102 came to light following the enactment of a California data breach disclosure law that
103 went into effect in 2003.

104
105 Consistent with NCSL's general policy for safeguarding financial information, NCSL
106 does not oppose baseline federal data security breach notification standards, provided
107 that the requirements do not preempt state authority to adopt standards that provide
108 affected consumers additional protection and notification. NCSL also supports allowing
109 state financial regulators and attorneys general to enforce any new federal data security
110 breach notification standards.

111
112 In the event that Congress decides to preempt state law, NCSL urges that the
113 preemption be narrowly construed to preempt only state laws that are inconsistent with
114 the federal standard while preserving state laws that apply to entities that may be
115 excluded from the federal act. Additionally, should Congress decide to preempt state
116 data security breach notification laws, NCSL would support a strong federal law that
117 would require notification of the affected consumers when sensitive personally
118 identifiable information has been, or is reasonably believed to have been, accessed or
119 acquired. In this instance, exceptions should be made only when it is concluded that

120 there is no significant risk that the breach has resulted in, or will result in, harm to the
121 individual whose information has been breached.

122

123 **Insurance Information Security**

124 In response to the GLBA requirements, state legislatures enacted operationally uniform
125 privacy protections for the nation's insurance consumers. In their role as the functional
126 regulators of the business of insurance, states have enacted numerous laws and
127 regulations that address the acquisition, retention, disclosure and use of financial
128 information by and among insurance companies. NCSL will oppose any federal effort to
129 preempt these state laws and regulations or to enact federal standards that address the
130 use of financial and credit information in insurance.