

DISCLAIMER

Electronic versions of the exhibits in these minutes may not be complete.


This information is supplied as an informational service only and should not be relied upon as an official record.

Original exhibits are on file at the Legislative Counsel Bureau Research Library in Carson City.

Contact the Library at (775) 684-6827 or library@lcb.state.nv.us.

Memorandum

To : Senate Committee on Commerce & Labor

From : J.J. Jackson, on behalf of the Consumer Data Industry Association (CDIA) 

Re : SB 379 (Credit File Freezing/Security Alerts)

Date : April 2, 2003

Chairman Townsend and Committee Members:

Attached hereto, please find copies of two position papers prepared by the Consumer Data Industry Association (CDIA), formerly known as the Associated Credit Bureaus. As you know, CDIA is the professional international association of more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening, and collection services.

Respectfully, CDIA and its members oppose SB 379. The first document attached hereto is an overview and analysis of SB 379, setting forth our opposition and reasoning therefore. The second document provides an overview of steps taken voluntarily by the consumer credit industry since 1993 to address, deal with, and remedy issues of identity and credit theft and fraud, and the results of those efforts.

Eric J. Ellman, Director and Counsel, Government Relations for CDIA, will hopefully be able to attend the hearing scheduled for April 4th, 2003. Alternatively, if Mr. Ellman's travel schedule will not allow for his personal appearance, we will endeavor to have other representatives from CDIA and its membership in attendance to present additional testimony. In the meantime, please feel free to contact me with any questions or concerns prior to the hearing at 702-460-6849.



Consumer Reporting Agency Responses to Identity Fraud

- 1993. Consumer Data Industry Association, then known as Associated Credit Bureaus, formed a Fraud and Security Task Force.
- 1998. Creation of True Name Fraud Task Force led by former Vermont Attorney General M. Jerome Diamond. The work of the task force included meetings with law enforcement, consumer organizations, privacy advocates, legislators and staff, victims, and others.
- The capstone of the True Name Fraud Task Force was a series of initiatives announced in March 2000. These initiatives meant the consumer reporting industry was the first industry to step forward and not only educate its members about the problems consumers experienced, but to seek specific changes in business practices. The initiatives are to:
 - Advocate the use and improve the effectiveness of security alerts through the use of codes transmitted to creditors. These alerts and codes can help creditors avoid opening additional fraudulent accounts.
 - Implement victim-assistance best practices to provide a more uniform experience for victims when working with personnel from multiple fraud units.
 - Assist identity theft victims by sending a notice to creditors and other report users when the victim does not recognize a recent inquiry on the victim's file.
 - Execute a three-step uniform response for victims who call automated telephone systems: automatically adding security alerts to files, opting the victim out of prescreened credit offers, and sending a copy of his or her file within three business days.
 - Launch new software systems that will monitor the victim's corrected file for three months, notify the consumer of any activity, and provide fraud unit contact information.
 - Fund, through CDIA, the development of a series of consumer education initiatives through CDIA to help consumers understand how to prevent identity theft and also what steps to take if they are victims.
- 2001. CDIA announced a police report initiative so that when a police report is provided as part of the process of disputing fraudulent data, Equifax, Experian and TransUnion will block these disputed items from appearing on subsequent consumer reports regarding that individual.
 - "Another collaborative effort with tremendous promise is your new police report initiative...I appreciate that certain consumer-based initiatives require you to balance accuracy issues - knowing that the consumer's report contains all relevant credit

information, including derogatory reports - against customer service. From my perspective, your police report initiative strikes just the right balance." *J. Howard Beales, III, Director of the FTC's Bureau of Consumer Protection, before the Consumer Data Industry Association. Jan. 17, 2002.*

- 2002. ID Fraud Victim Data Exchange. CDIA and its members committed to start a pilot test in early-2003 so that when an ID fraud victim calls any one of the participating credit reporting agencies, the victim will be notified that his or her identifying information will be shared by the receiving credit reporting agency with the other two participating credit reporting agencies and that the following steps will be taken by each recipient of the victim's information:
 - A temporary security alert will be added to the victim's file. This security alert will be transmitted to all subsequent users (e.g., creditors) which request a copy of the file for a permissible purpose under the Fair Credit Reporting Act.
 - The victim will be opted out of all non-initiated offers of credit or insurance.
 - The CRA will ensure that a copy of the victim's file is in the mail within three business days of the victim's request.

- Our efforts are paying off.
 - *Most calls are prevention related.* CDIA members report a majority of consumers who contact fraud units are taking preventative steps and are not reporting a crime.
 - *Victims are learning of the fraud earlier.* According to an FTC report in June 2001, 42% of victims learn about the crime within 30 days or less, a full 10% less than than in the prior report. CDIA estimates another 35% learn of the crime within one to six months and 7% learn of the crime in six months to a year.
 - *Victimization of the elderly is dropping.* In 2001, the FTC estimated that 6.3% of identity fraud victims were over 65, a 5% decrease from 2000.

About CDIA

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus (ACB), is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

For more information about CDIA, its members, or identity fraud or other issues, please visit us at www.cdiaonline.org or contact us at 202-371-0910.

March 2003



**Nevada S.B. 379 (File Freezing/Security Alerts)
Position: OPPOSE**

Legislative Proposal: Senate Bill 379: (1) allows consumers to place security alerts on their credit reports, §§ 10, 12-13, (2) allows consumers to freeze access to their credit reports, §§ 11, 14-19, and (3) makes other changes to existing credit reporting law, § 21. Most of the bill is based on California law, including file freezing. File freezing, the most dramatic alteration of the credit reporting system in its history, has only been in effect in California since January 1, 2003.

Current Law: The federal Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*) has governed the nation's credit reporting system since 1971 and was modernized in 1997. This comprehensive law, which was also the first national privacy law in the United States, places strict limits on who can access credit information and under what circumstances, allows consumers to obtain their credit reports at any time, and affords them an opportunity to dispute information they feel is inaccurate. In Nevada, CDIA members are also governed by the Nevada credit reporting law, NRS Ch. 598C. This law mirrors federal law in many respects.

Current Marketplace: The consumer reporting industry has a number of voluntary initiatives in place nationally to benefit consumers, including victims of identity fraud (see attached). These voluntary initiatives for identity fraud victims include the placement of a fraud flag on a consumer's report, and the blocking of fraudulent tradelines on consumer reports. The consumer reporting industry is strongly committed to preventing identity fraud in the first place and assisting those consumers who have been victimized.

Reasons for Opposition: Codifying voluntary initiatives that are working only serves to discourage the consumer reporting industry from innovating. Identity fraud is a high-tech fast, fast-moving crime where the consumer reporting agencies always have to be one step ahead of the bad guys. Mandating a specific response which makes little sense today, may make even less sense tomorrow. Additionally, the security freeze proposal is the most dramatic and draconian alteration to the credit reporting system since the American system was first established in colonial times.

1. Sections 10, 12-13. Security Alerts. This section would require consumer reporting agencies to allow consumers to place security alerts on credit files. A law is not necessary to require the addition of security alerts on consumer reports. Today, Equifax, Experian, and TransUnion voluntarily add security alerts to any consumer's file when that consumer identifies him- or herself as an identity fraud victim. Once posted to a credit report, security alerts are transmitted to all subsequent users of the consumer's report. The alert stands as a flag to alert all credit grantors that the credit report is associated with a fraud victim and additional steps may need to be taken to confirm the identity of the applicant. The voluntary practices outlined here make sense for the consumer credit reporting industry, for creditors, and for consumers who are victims. There is no evidence that the voluntary efforts of CDIA members are not working today. Additionally, the bill will erode the effectiveness of the alerts by flooding the system with false alerts not tied to an incident of some type, like a lost wallet.

2. *Sections 11, 14-19. Security Freezes.* This section of the bill requires consumer credit reporting agencies to operate a system where they must accept a consumer's written request to place a "security freeze" on his or her credit report. The net result of this freeze is that no information may be provided to a third party except with the consumer's express authorization. The consumer's request must be honored within five business days after receipt and a written confirmation of the placement of the security freeze must be sent to the consumer within 10 days of the freeze becoming effective. The notice to the consumer shall include a "unique identification number or password" to be used by the consumer to authorize release of the credit report. A security freeze remains effective until a request is made by the consumer for removal and proper identifying procedures have been followed.

Security freezes are law in no place other than California and in California the law has only been in effect for a few months. As mentioned above, this is a major and serious alteration to the credit reporting system, which works, according to FTC Chairman Tim Muris, because:

Without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide - on a creditor-by-creditor basis - whether they wanted their information reported, the system would collapse.¹

It is too early to predict if the California experiment is really working and no state should rush headlong in to adopting the experiment until there is able evidence it is actually working. Already, the file freeze appears to be hurting some mortgage applicants. Fannie Mae, a major force in the mortgage process, has recently published a policy that:

Credit reports that are incomplete due to frozen credit are not acceptable for underwriting with Desktop Underwriter[®] (DU[™]) or for manually underwritten loans. Furthermore, nontraditional credit reports are not an acceptable alternative to incomplete credit reports due to frozen credit data.²

This new policy could delay by days or weeks the decision process about whether a consumer's mortgage application is ultimately approved. This crucial delay is at best an inconvenience to consumers and at worst, it could cause them to lose their dream home.

Below are some examples of practical problems associated with the bill.

- **Online Shopping.** Consumers find the Web an excellent tool for comparison-shopping. Consider the following consequences to all forms of online comparison shopping based on the following examples:
- **Mortgage Shopping Online & File Freezes**
 - The bill requires that the consumer direct the consumer credit reporting agency in advance of the transaction to release the file, which has been "frozen" by the consumer. How will the consumer do this if they are shopping online for a loan via a multiple-lender shopping website? The very nature of e-Commerce suggests that consumers shop for loans by first using browsers to list potential sites on which they

¹ FTC Chairman Tim Muris, Oct. 4, 2001. before the Privacy 2001 Conference in Cleveland.

² <http://www.efanniemae.com/singlefamily/technology_tools/information_providers/ca_credit.jhtml#underwriting> (visited Feb. 7, 2003).

may wish to shop. Does the bill contemplate that the consumer will then proceed to the sites, determine which ones he/she truly want to use for a loan, then print out these home pages and then contact the consumer credit reporting agency to seek to have his/her file released?

- **Automobile Shopping Online & File Freezes.** Similar to the mortgage loan shopping example, does the bill contemplate that consumers must first "pre-shop" online and then contact the consumer credit reporting agency to seek release of the file for those sites where the consumer is likely to do business?
- **Cellular Phone Customers & File Freezes.** Consumers apply in-person and on the Internet for cellular phone service. In either scenario, it is unlikely that consumers will know which services they intend to visit and thus, in advance, "unfreeze" their file.
- **New Online Checking Account/Banking Services Applicants & File Freezes.** Where consumers wish to open a new checking account they will have to know in advance which depository institutions they intend to visit online in order to unfreeze a consumer credit report which is often used for fraud prevention by the institution. Absent access to checking account fraud and traditional credit reporting databases, the depository institution may simply be unable to approve the opening of a new account. Consumers who make application via an ATM or the Internet will be affected, as well.
- **Insurance Applications & File Freezes.** Many types of insurance underwriting are tied with use of a consumer's credit report. Consumers who have "frozen" their files won't likely know in advance with whom they will apply for insurance and thus won't be able to "unfreeze" a file prior to shopping for better rates. This is true whether the consumer is shopping via an agent or the Internet.
- **Online Identity Authentication and Verification.** Internet fraud is of great concern to consumers and to industry. Properly identifying customers and reducing fraud is key to the success of electronic commerce. Today, properly identifying consumers is easily achieved through the use of consumer credit reporting products and electronic signature transactions. These identity verification products are consumer credit reports and are designed for a wide range of e-Commerce retailers and other companies, which have a need to verify the identity of consumers before completing a transaction or delivering a product. Consumers won't always even be aware in advance that a traditional online retail transaction may involve the use of identification products tied to consumer credit reporting agencies and thus won't know to "unfreeze" their file for Internet shopping in general.
- **Online Credit Card Transactions.** Today, an e-Commerce site has at least two concerns where they are completing a transaction. They want to ensure that the credit card account information is valid and they want to make sure that the person entering the credit card information is in fact the account holder. Credit reporting systems are the key supplier of what are often referred to as "out of wallet tests" to validate that the credit card account is being used by the account holder by requiring the consumer to respond to a series of questions about their financial transactions such as which mortgage lender holds their loan. By asking these questions, criminals are thwarted in their attempt to use stolen credit card account information. VISA just made a commitment to this "out of wallet" test in June of 2001.

In the bricks-and-mortar world of shopping, similar examples to those of e-Commerce can be drawn such as a consumer shopping at a series of auto dealers and not knowing in advance which lender will provide the financing. How will the consumer "unfreeze" a file when they won't know the name of the lender financing the car, the furniture or the home? The number of lawfully permitted and valued uses of consumer credit reports in combination with the range of media used to deliver these reports and the number of instances where the complexity of the decision is high due to the number of users involved renders this legislative proposal unworkable. To clarify further, unlike an ATM network, there is no single technology platform on which to administer a personal number or identifier. The proposal contemplates a web of systems of authorization (some requiring complex authorizations involving multiple parties) across a host of media (telephone, Internet, even mail?) and for a myriad of different industry sectors.

- **Gaming Impact.** The gaming industry uses consumer reports to (a) check the backgrounds of prospective employees, including cashiers, dealers, and security personnel, and (b) check the credit of some customers. A consumer who has frozen his or her file might be able to "credit repair" that file³ to remove information like liens, judgments, or bankruptcies, or records of arrest or conviction and then unfreeze the best credit report. The result is the applicant for a position as a cashier appears to be a far better risk than she might otherwise be. The same scenario applies to customers of the casinos or any other credit customer or job applicant.

In addition to the extreme complexity of the proposal, empowering consumers with the option to freeze files will expose the financial system to even greater risk of credit repair agencies which promise to assist consumers in engaging in what the Federal Trade Commission terms "file segregation." This scheme proposes to consumers that, for example, they avoid their current accurate credit history, which has accurate derogatory information, by applying for an employer identification number from the Social Security Administration and then using this number in combination with a postal box and perhaps a slightly altered name to apply for new credit or other services. The new identifying information prevents the lender or other service provider from reviewing the consumer's true credit history and thus credit is granted to a consumer who is already having problems paying on current obligations. This misuse of the Social Security Administration EIN system as well as providing advice, which encourages consumers to perpetrate fraud, is exacerbated where consumer can block use of the credit history.

The proposal for security freezes contemplates preserving use of the consumer's credit report through exceptions to the freeze where there exists some type of current business relationship. Our members' concerns about liability for unauthorized release of the file will lead to dramatic reductions in access even where such relationships exist. Today, federal law already limits the permissible uses of a consumer's file. The consumer credit reporting agency will have no ongoing means of monitoring when and how a consumer relationship changes or ends with regard to a particular business. This proposal may even interfere with the review of insurance and credit portfolios where review of individual files is permitted under the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

³ "Everyday, companies nationwide appeal to consumers with poor credit histories. They promise, for a fee, to clean up your credit report so you can get a car loan, a home mortgage, insurance, or even a job. The truth is, they can't deliver * * * [Even though credit clinics might claim to be able to, n]o one can legally remove accurate and timely negative information from a credit report." Credit Repair: Self-Help May Be Best, Federal Trade Commission <<http://www.ftc.gov/bcp/online/pubs/credit/repair.htm>> (viewed March 31, 2003).

More fraud prevention technologies are being deployed to better identify patterns of fraud and to better identify consumers, including use of biometrics. Fraud is not effectively prevented by a rigid legislative mandate, which targets a particular tactic or technology. The crime of identity fraud is prevented by the layering efforts including effective enforcement of crime statutes, the deployment of fraud prevention/detection technologies, sound policies, the right training for personnel and consumer education.

The bill prohibits release of information from a consumer's credit report without prior express authorization from the consumer. This prohibition may result in our inability to use the credit information, stripped of any personal identifying information, in score development. Today, credit reporting databases are used to create risk models for many credit and insurance applications. The existence of these risk models benefits consumers in many ways, including more competition among financial services companies and insurance underwriters, and more choices and lower rates for most consumers. If Nevada were to adopt a file freezing statute, it would be very important to exempt such important uses of the data stripped of individual identifying information.

3. Section 21. Additional Changes to Existing Law. Federal and Nevada credit reporting laws have worked well for a long time and there is no evidence that amendments are necessary. The changes contemplated by Section 21 are already covered by existing federal law and under that federal law, any Nevada resident can sue a credit bureau in state or federal court. The Nevada attorney general can also sue a credit bureau under federal law in state or federal court. Finally, the FTC can also sue a violating credit bureau.

Conclusion: Codifying fraud responses based on voluntary initiatives stifles creativity and innovation and does a disservice to consumers. Additionally, the dramatic changes to credit reporting operations are unwarranted. Finally, the bill would make an immediate change to an untested California law that dramatically alters the long-standing and efficient credit reporting and granting systems. The impact of the bill will be severe to consumers and businesses alike and should be very carefully scrutinized.

About CDIA:

Founded in 1906, the Consumer Data Industry Association (CDIA), formerly known as Associated Credit Bureaus, is the international trade association that represents more than 400 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

For More Information:

Eric J. Ellman, Director and Counsel, Government Relations

Phone: 202-408-7407

Email: eellman@cdiaonline.org