P. O. Box 512
Montpelier, Vermont 05601
January 18, 2018

House Committee on Commerce and Economic Development
State House
Montpelier, Vermont

Subject: Data Broker Committee Bill

Dear Committee Members:

Please consider this letter as testimony on this bill. I am working from draft no 5.1.

I think that the draft bill has some serious deficiencies and I ask that you correct them. I use the term "I think" as a request to you to make a change to the bill.

general comments

247,000 Vermonters should not have to request a security freeze. I think that the data broker should be required to automatically place a security freeze on all breached accounts and notify each affected Vermonter that a freeze has been placed, why the freeze has been placed, and the steps to undo the freeze on a short-term basis and on a permanent basis. The onus for reducing the damage cause by the holder of the data should be on the holder of the data rather than on the consumer whose data have been breached.

I think that data brokers should be liable for damages to Vermonters whose data have been breached.

The bill does not cover the case of a data collector using data for a purpose other than that for which it is collected. An example is my high school class. We are now preparing for a class re-union. As part of that preparation the class has hired an on-line service to take submissions from classmates on their activities since graduation. The plan is to then have a book compiled with that information. I think that the bill should prohibit that company from selling or otherwise using that data for any purpose other than the book. The definition highlighted in yellow (page 14, lines 11 through 15) seems to provide this protection to consumers from a data broker but not from a data collector.

If a credit agency cannot maintain personal information securely, I have no reason to believe that the same agency can protect a unique personal identification number or password. This refers to the personal identification number or password given out when a consumer requests a security freeze (page 10, lines 5 and 6; page 55, lines 11 and 12; and page 59, line 15). I have no idea of a potential solution that protects consumers. Perhaps a solution would be to prohibit that agency from collecting, maintaining, or providing information about any consumer whose data the agency allowed to be breached. After all, there are other credit reporting agencies, so the affect on the consumers is not so drastic as if there were no alternatives.

specific comments

Definitions in §2480a (chapter 63, consumer protection, subchapter 3, fair credit reporting) and §2430 (chapter 62, protection of personal information, subchapter 1, general provisions) (page 14, line 8) are different. The definition in §2480a is "a natural person residing in this state". Yet it seems that much of the data broker chapter takes text from the fair credit reporting subchapter. I think that you should look into the necessity for different definitions and make them the same if feasible.

The bill proposes to define a data broker (p. 14, lines 9 through 17) as a business that does not otherwise have a direct relationship with a consumer. I think the bill should make sure that requesting a credit report or requesting to have a security freeze placed does not then create a direct relationship with the business.

The bill proposes to cover only the sale of personal information (p. 14, line 9). I think the verb should be "sells or transfers".

Sale of personal information on minors is on an opt-out basis (page 20, lines 8 and 9 and lines 18 and 19). I think this should be changed to an opt-in condition, to provide more protection. I also think that the verb here should be changed to "sale or transfer" instead of merely "sale".

The lengths of time before notification (p. 22, lines 1 through 11 and page 44 lines 5 through 11) are unreasonably long and provide little protection to a consumer. I think that consumer protection requires consumer notification to have priority over law enforcement. I think that a delay of up to 45 days is way too long for the data broker to repair the faults in the system that led to the data breach. I think that a hold by law enforcement beyond 45 days is unreasonable. If I read these lines correctly, a hold by law enforcement can last indefinitely long beyond 45 days. That is no protection to a consumer.

I think that consumers should be notified by certified mail. The burden on the data collector who has failed to protect the data needs to be enough to act as an incentive to prevent the security breach in the first place.

I think that the specified period of time is too long. I think that the data collector's first responsibility in event of a security breach is to notify the consumers whose data have been breached. This notification should have priority over law enforcement investigation. I think that the consumer needs to know immediately, in order to be able to take steps to prevent (or at least reduce) damage from the breach.

I think that the placing of consumer notification at the bottom of the list of notification priorities is too disrespectful of a consumer's need to know of a data breach. Notice of a breach to each consumer should not be delayed for law enforcement or for repair of the breached system.

How can a data broker have regular communication with a consumer? This refers jointly to the definition of a data broker (not having a direct relationship with a consumer) and the ability for electronic notice (page 28, lines 8 and 9 and page 49, lines 1 and 2). It seems that regular communication implies a direct relationship, therefore is not covered by this bill.

The bill allows for a data collector to give telephonic notice (page 28, lines 16 and 17 and page 49, lines 11 and 12). The bill does not appear to provide any way for a consumer to know that the telephone call is not a scam. I think that telephonic notification should be prohibited unless there is some mechanism by which the consumer can be assured that the telephone call is legitimate. I think the bill should also contain prohibitions on requests for a consumer to take action based on the telephone call. (Otherwise the chance of a consumer getting caught by a scam increases greatly.)

The terms for a substitute notice (page 28, line 18 through page 29, line 8 and page 49, line 13 through page 50 line 3) are woefully inadequate. $5000 divided by 247,000 Vermonters yields 2 cents per Vermonter. If that's the only cost, there is little incentive to protect data. I think that the entire possibility of substitute notice should be stricken from the bill. I think that the data broker should be required to notify each affected consumer individually and in writing.

The bill proposes to limit safegaurds to the amount of resources available to the data broker (page 38, line 17). I think that this should be stricken. I think a data broker with a large amount of data should not be allowed to evade its responsibilities through manipulation of the corporate structure or manipulation of financial arrangements.

The bill is really vague about how secure the information security program (pp. 41, line 6 through p. 43 line 7) needs to be. That is because it uses the word "reasonably" numerous times. I think that instead of "reasonably" it should be more like "the most recent" or perhaps "daily updates, with more frequent updates necessary when I

really bad problem is found". You can convert that into legalese and make adjustments for each appearance of "reasonably". I'm referring for example to the problems recently announced with microprocessor chips. Updates have then been released to work around the problem. Using the qualifier "reasonably" does not require the data broker to install those updates as soon as released. Also, what a data broker considers to be reasonable is likely to be far different from what you think is reasonable.

My latest directory has 10 listings in the yellow pages under Credit Reporting Agencies. Not all of them are listed in the white pages. I think the bill should be amended (page 52, lines 13 through 15) to ensure that the listings are in the yellow pages under both credit reporting agencies and data brokers.

The purpose of the exception in the notice relating to direct mail offers of credit (page 53, line 15) is not clear. I think it is a huge loophole. It means that someone could establish a company to offer credit by direct mail. The company could then get credit information from each reporting agency without the permission of the consumer. I think that this should be removed from the list of exemptions to accessing a credit report.

The term "pre-authorized approvals of credit" is not defined (page 56, line 14). In addition, pre-authorized approvals of credit are not listed as an exemption. So it is not clear why a security freeze will not apply to pre-authorized approvals of credit. I think that this exemption should be eliminated.

The bill retains time limits for written notification of security freezes (page 59, lines 13 through 19). Is the limit 10 business days from receiving the written notice or 10 business days from placing the freeze? I think that this should be clarified to be "the earlier of 5 business days from placing the security freeze or 10 business days from receiving the written request from the consumer." This keeps the time limited in case the agency misses the deadline for placing the freeze.

summary

In summary, some aspects of this bill do more to protect data brokers rather than to protect consumers whose data have been breached. I ask that you alter those sections to provide more protection to consumers. All of the "I thinks . . ." are a request for you to change the bill.

Thank you for taking time to read these comments.

Sincerely,

Thomas Weiss