P. O. Box 512
Montpelier, Vermont
April 10, 2018

Senate Committee on Economic Development, Housing, and General Affairs.
State House
Montpelier

Dear Committee:

Good morning, I am Thomas Weiss, a resident of Montpelier who meets the definition of a consumer. I am testifying on H-764, data brokers and consumer protection. I think that protection of personal information is important, and I thank you for allowing me to present my thoughts on this subject. These comments are from my point of view as a consumer. I bring my experience as a civil engineer to this testimony. As a civil engineer, I have had to read and to know and to understand laws, regulations, and contracts my entire career in order to do the engineering that I do. I use that background to help me figure out and understand what this bill does and does not do. I find this bill and the underlying statutes to be confusing. I find that the bill and the underlying statutes protect the entities that handle a consumer's data more than they protect consumers.

My goals
- To increase the accountability to consumers by those that handle data.
- To increase the number of paths by which consumers are directly notified of unauthorized acquisitions of data.
- To reduce the number of conditions that allow authorized acquisitions of data.
- To make the data broker provisions useful to consumers.

What this testimony covers
- The findings and intent of the bill
- The data elements being handled and the entities that handle them
- Relationships among categories of data handlers
- Prohibitions on data trafficking and §2433
- Increasing the number of paths for consumer notification of unauthorized data acquisitions.
- Why provisions governing data brokers are unfriendly to Vermonters
- Security freezes.
- How consumers are kept in the dark about authorized acquisition of data
- Establishing liability for data handlers

The stated purpose of the bill is "to adopt consumer protection provisions relating to data security and consumer privacy." The part on security freezes enhances consumer protection. The part on prohibiting some acquisitions of personal data enhances consumer protection. The rest fails to meet its purpose. The bill protects data brokers at the expense of consumers. And the underlying statute was not strengthened to improve data security and consumer privacy relating to data collectors.

The findings and intent of the bill. (Sec. 1)
The portions of the bill that amend chapter 62 (protection of personal information) focus narrowly on data brokers. The findings and intent of this bill create this narrow focus. Thus, the bill misses opportunities to take advantage of the broader purpose of the bill to strengthen consumer protection.

The findings of the bill
One finding is about providing consumers with more information about data brokers, their data collection practices, and the right to opt out. Testimony given to the House Committee on Commerce and Economic Development from just two trade associations indicates 1700 members. A check in my most recent (2016) Fairpoint telephone directory finds 10 credit reporting agencies. Even if only a fraction of them register and

handle data on Vermonters, it is unrealistic to expect that consumers will have the tenacity to review the registration site for more than a few.

Another finding is that "Data brokers provide information that is critical to services offered in the modern economy". However, there is a difference between "critical to services offered in the modern economy" (as in the bill) and "services critical to the modern economy" (for which there is no finding). None of the services listed in the finding are services critical to the modern economy.

The bill has a finding that talks about risks relating to a consumer's ability to control information held and sold about the consumer or arising from unauthorized use of consumer information. The bill does not follow through on this finding. The bill gives consumers no mechanism for authorizing or controlling use of their data, once they have given the data to a data collector.

Proposed additional findings

- Handlers of data collect data about a consumer directly and indirectly. Many handlers of data get their data both ways. Thus, the boundaries among data collectors, data brokers, and destroyers of data records are indistinct. A given entity can be all three types of data handler simultaneously.
- Portions of the underlying statutes are weak on protection of personally identifiable information and inhibit notice to consumers. Strengthening those portions of the underlying statutes will benefit consumers.
- Some data elements are not marketable commodities. They are not to be bought and sold. These are the data elements that an individual uses to establish his or her identity. The transfer of data elements that are not marketable commodities should be defined as "data trafficking" and made a crime.
- It is specious to argue that consumers who "voluntarily" provide data have meaningful control over how the data are used.
- It is unconscionable to expect all Vermonters to have to worry about credit ratings and identity theft when as few as 5,001 have had their data stolen.
- Existing statute requires direct notice to consumers only if the cost to the data collector does not exceed $5,000. The resulting shift in cost burden to all Vermonters to investigate whether they are the ones who have been affected will far exceed $5,000.
- Data are data, no matter the form. It matters not to a consumer whether an unauthorized acquisition is on paper or through electronic files. It is now easy to convert paper documents into searchable digital forms.
- Consumers are kept in the dark about too many acquisitions of data, whether they be authorized or unauthorized. In too many instances when the acquisition is unauthorized, either the consumer never learns of the unauthorized acquisition or the consumer is not notified directly that the acquisition includes his or her data. Even when a data handler authorizes an acquisition, that is often without the knowledge or express consent of the consumer.

The intents of the bill

- Providing consumers with more information regarding data brokers.
- Ensuring that data brokers have adequate security standards.
- Prohibiting the acquisition of personal information with the intent to commit wrongful acts.
- Removing financial barriers to protect consumer credit information.

The additional findings proposed above lead to a need for additional intents.

Proposed additional intents

- Giving the consumer more control over the use of the consumer's personal data.
- Increasing the paths leading to direct notice to consumers of unauthorized acquisitions of data.
- Declaring that the marketing of some data elements is unacceptable.
- Preventing the re-purposing of data obtained directly from a consumer

The data elements being handled and the entities that handle them (§§2430, 2433, 2440)
I think the bill and the statutes will be easier to understand if they focus on the data elements and not on the names given to data handlers. With the focus on the data elements, there is no need to create different categories of data handlers. If an entity is handling personally identifiable information, the entity and the information are subject to one set of requirements. If the entity is handling personal information, the entity and the information are subject to a second set of requirements. If the entity is handling confidential information (if you choose to keep this grouping of data elements), then the entity and information are subject to a third set of requirements.

The data elements that are included in each of the three groups are shown on exhibit 1. Exhibit 2 is my proposal for an amended grouping of data elements into two groups. The two exhibits show all data elements mentioned in bill H-764.

Exhibit 1 shows the data elements as classified by H-764. These groups are "personal information", "personally identifiable information", and confidential information". Looking at how the data elements are assigned, I sense some confusion concerning the type of data element that belongs in each category. One example is a driver's license number. It seems odd to me that the bill does not require it to be treated the same by all data handlers. For example, whether or not a consumer is notified of a breach of the driver's license number depends on whether it is being held by a data collector, a data broker, or a destroyer of data records. Or whether it is in digital form or paper form. Or whether it is encrypted or not. Destroyers of data records have to protect the information in any form, digital or not, but they need not report an unauthorized acquisition. This means that a data collector need not protect this personal information when it is in non-electronic form and must protect it during the process of destroying the records containing the information.

Exhibit 2 shows the data elements as I propose them. This exhibit places the data elements into two groups and re-arranges them. One group is the personally identifiable information, the other is the personal information.

It is not clear why some data elements are included in personally identifiable information and similar data elements are included in personal information. The identification numbers are one example of this split. that are similar to ones included in personally identifiable information are not there and are in personal information instead. I think that many of the elements in personal information in the bill really need to be treated as personally identifiable information.

Personally identifiable information, as used in my proposal in Exhibit 2, contains data elements that I suggest should be obtained only directly from a consumer. These data elements are of the type used to establish a person's identity or are those relating to bank accounts and the like.

Personal information, as used in Exhibit 2, contains the other data elements mentioned in the bill.

If this bill is enacted, it will mean that the State thinks it is perfectly acceptable that personally identifiable information is a marketable commodity; a commodity that may be bought, sold, disseminated, obtained, or transferred by anyone else. I do not understand why that is acceptable. I suggest that engaging in such activities should constitute a crime of data trafficking. An example is a passport number. I suggest that data trafficking be applied to all data elements included in my proposed category of personally identifiable information in Exhibit 2. I also think that consumers should be notified when there has been unauthorized acquisition of those data elements. Thus, I propose that certain data elements be removed from the definition of personal data. Those items are listed as "no" in exhibit 2 and highlighted in gray, to show a change from exhibit 1. Whether or not you agree with my concept of data trafficking, I urge you to accept my grouping of the data elements.

I do not understand why certain elements are not classified as personally identifiable information. For example, the bill classifies a biometric record as personal information. It seems that personally identifiable information is a more secure classification for biometric records. A biometric record and some other data elements should be classified as personally identifiable information. Those elements are listed in exhibit 2 as "yes" for personally identifiable information and highlighted in gray, to show a change from exhibit 1.

Proposed amendments to the bill

- Adopt the proposed classification of data elements as shown in exhibit 2.
- Add additional data elements to the list of personally identifiable information. Some of these elements would come from those that are determined to be exempt from disclosure as public records. (Not all of the public records exemptions, but there are some that could be added to the list.)
- Determine how to handle data elements that are not listed in Exhibit 2.
- Create the crime of data trafficking for personally identifiable information and add it to §2433.
- Change the term "personally identifiable information" to "confidential information to more accurately reflect the nature of the data elements.

Relationships among categories of data handlers (§§ 2430, 2435, 2445, 2446, 2447)

The bill covers multiple types of data handlers and omits other types of data handlers. The bill covers data collectors, data brokers, destroyers of data records, and the multiple entities contained in §2440 (Social Security number protection). The definitions of these types of data handlers depend on the type of information that they use, their sources of the information, and what they are doing with the information. The bill omits coverage of data handlers that deal with personal data elements that are neither personally identifiable information nor personal information nor confidential information. The bill omits coverage of data handlers that deal with non-digitized data, or with encrypted digitized data.

The boundaries defining data collectors, data brokers, and destroyers of data records are fuzzy. An entity can at different times be all three. The bill does not explicitly state that a given entity can be subject to the requirements of all, depending on the type of information and what the entity is doing with the information. However, if the focus is on the data and data elements, then the fuzziness that develops by following the category of the entity (instead of the data elements) disappears.

One example is when data collectors and brokers hire companies to destroy data records. The destroyer of data records likely is destroying records that contain data elements from all three groupings: personally identifiable, personal, and confidential information. Because the destroyer of data records handles personally identifiable information, it is a data collector. Because the destroyer neither sells nor licenses the personal information, it is not subject to the conditions that apply to personal information. Is that what is intended?

Another example is retailers. They are data collectors when they collect personally identifiable information from consumers. Some retailers also collect personal information.

- If retailers collect personal information from the consumer and then sell that personal information, they will not be governed by the provisions relating to data brokers. Is that what is intended?
- And what happens when the retailer collects personal information from a source other than the consumer and then sells that information? Does that make the retailer a data broker? It is not clear, because the retailer has a direct relationship with the consumer, although not for those personal data elements.

Proposed amendments to the bill

- Focus on the data elements and not on the category of the entity handling the data.
- Or, explicitly state that a given entity that performs activities of more than one type of data handler must meet the requirements for all of those types of data handlers. Thus, when a given entity meets the definition of a data collector it must comply with those provisions. If it also meets the definition of a data broker it must also comply with those provisions. And if it also meets the definition of a destroyer of data records, it must also comply with those provisions.
- Review the definitions of the categories of information and of data handlers. Then make sure that their are no gaps that should be covered.

Prohibitions on data trafficking and §2433

Prohibitions on acquisition of data are contained in §2433 of the bill. The prohibitions there are both important and insufficient.

The bill prohibits acquisition of personal information through fraudulent means or for nefarious purposes. The bill does not extend the prohibitions to personally identifiable information. That likely means that it is acceptable to acquire personally identifiable information through such means or for such purposes.

Many data handlers collect data from a consumer ostensibly for one purpose and then have no restrictions on using it for another purpose. Consumers might or might not have control over that. I give two examples. The first involves the bankruptcy of a large company a few years ago. News reports stated that the company's most valuable asset was its data base of customers. If the company did indeed sell its data base, then that is an example of re-purposing. Another example is a class re-union. The class decides to contract with an on-line site for a book. Class members can provide brief sketches of their lives since graduation. If that company then transfers the data to another entity or sells the book to non-classmates, that would be re-purposing.

Some data elements are too sensitive to be marketable. We should declare it to be unacceptable to include them in a transfer of data; unacceptable to treat them as a marketable commodity. If a data handler truly needs to have this information, it will need to get the information directly from each consumer. I have proposed above to place these elements into the group of personally identifiable information.

Just because a consumer has a direct relationship with a data collector does not mean that the consumer knows about the data collector's other activities. The consumer likely does not know what data the collector obtains from other sources and what the collector does with any of the data. Privacy policies often are written broadly, to the effect: we reserve the right to disseminate your information for any legal purpose. That is unenlightening to consumers other than as a warning that the data collector will disseminate the data as much as possible: that is without restriction unless prohibited by law. Such a privacy policy allows unlimited re-purposing.

Proposed amendments to §2433 of the bill

- Expand the prohibitions to add the category of personally identifiable information where §2433 already has personal information.
- Prohibit the re-purposing of data collected directly from a consumer, unless specifically authorized by the consumer. Using privacy policies or similar requirements authorizing re-purposing of data in order to obtain a service would be prohibited. This also includes prohibiting a retailer that obtains information from a consumer in connection with an on-line purchase from selling that data or using it for any other purpose than for on-line purchases with that consumer.
- Make data trafficking a crime, which would be the buying, selling, transfer, etc. of personally identifiable information. The only legal way for a data handler to get personally identifiable information would be to receive it directly from the consumer.

Increasing the number of paths for consumer notification of unauthorized data acquisitions. (§2430, 2435, 2446, 2447)

Unauthorized acquisition of personally identifiable information

The provisions on unauthorized acquisition of personally identifiable information apply to all data collectors. The provisions do not apply to data brokers. A flowchart of the notice provisions is shown on exhibit 3. The important point of this flowchart is that there are many more pathways for data collectors to keep consumers in the dark about unauthorized acquisitions of data than for data collectors to actually notify consumers.

Eight out of the ten paths on the flow chart keep consumers in the dark. Only two paths lead to direct notice to consumers of an unauthorized data acquisition.

Consumers are the last to learn of a security breach. The order of receiving information is: data collector; attorney general (or department of financial regulation); law enforcement; and eventually consumers. By making the consumers the last to know, the consumers lose valuable time before they can begin to take steps to prevent (or at least reduce) damage from the breach. This is disrespectful of a consumer's need to know of an unauthorized acquisition.

In addition, the lengths of time before notification are unreasonably long. The bill will allow the data collector to withhold notification up to 45 days. Law enforcement may delay notification indefinitely. These factors increase the risk to consumers of damages or identity theft due to the unauthorized acquisition. The consumer will not be able to take timely action to mitigate the consequences of the collector's failure to protect the consumer's data. Such a long delay in providing direct notice to consumers also places the interests of the data handlers above the interests of consumers.

The bill will allow direct notice to a consumer to be done in writing, by telephone, and electronically. It is risky to rely on telephonic notification or electronic notification, because of the prevalence of scams using those media. The bill does not appear to provide any way for a consumer to know that the telephone call or the e-mail is not a scam. The type of requests that the data collector would make to notify a consumer in a telephone call or e-mail are the same type that are involved in many scams. The consumer has no way of knowing whether such a notification is legitimate or a scam.

Data collectors are not required to notify anyone when the data are on paper or in another non-digital form. I do not understand why only digital data are covered. Identity theft is identity theft, no matter whether the information allowing that theft was obtained in digital form or in paper form. The individual whose identity has been stolen, or who has been damaged, probably will not feel better because the information was in paper form.

A number of internet sites contain pre-digital paper records that have been converted into searchable digital files. The ones that I have used include technical reports, newspapers, and encyclopedias. An unauthorized acquisition of paper records, then converted into digital files, provides little protection to consumers. Yet paper records are excluded from the requirements for data protection and notice to consumers for unauthorized acquisitions.

Data collectors are not required to notify anyone when the data are protected by encryption, redaction, or another method.

- Yet the bill fails to define the levels needed to meet this standard. Weak protection will meet the terms of the bill, will let the data collector off the hook when there has been unauthorized acquisition of the data, and will leave the consumer in the dark.
- Even if the data are encrypted, redacted, or otherwise protected at the time of the breach, it is only a matter of time before a determined data thief will crack the protection and have full access to the data.

The use of the verb "license" seems to mean "granting permission to use data" in some places and "receiving permission to use data" in other places. For example, §2435(b)(2) is particularly confusing, because it seems to have inverted the meanings of the word. In my dictionary the verb "license" means "to issue a license to". And one that has a license is a "licensee".

The bill allows a data collector to avoid any notice to consumers by establishing that mis-use is not reasonably possible. The bill leaves the definition of mis-use to the discretion of the data collector. What a data collector thinks is not reasonably possible could vary greatly from what a consumer thinks is not reasonably possible.

Allowing a data collector to use only substitute notice fails to hold the data collector accountable for the unauthorized acquisition. Whenever substitute notice is used, it means all Vermonters will have to use their own resources to determine if their data have been breached.

- The monetary limit for allowing a data collector to use a substitute notice (and avoiding direct notice) is woefully inadequate. $5,000.01 divided by 247,000 Vermonters yields 2 cents per Vermonter. If that's the maximum cost to a data collector, there is little incentive to protect data.
- The population limit of 5,001 for allowing a data collector to use a substitute notice (and avoiding direct notice) also is woefully inadequate.

Unauthorized acquisition of personal information

The bill has no provision that either consumers or the State will ever learn about an unauthorized acquisition of personal information (a data broker security breach). The most they will learn will be an annual summary due on January 31 of the number of security broker data breaches during the previous calendar year and the total number of consumers affected by the breaches.

Proposed amendments to the bill

- Notify consumers immediately of an unauthorized acquisition.
- Remove the ability of law enforcement to place a hold on direct written notice to consumers.
- Require all notices to consumers to be direct notices in writing and delivered by certified mail.
- Prohibit telephonic or electronic notice unless there is some mechanism by which the consumer can be assured that the notice is legitimate and not a scam.
- Expand the definitions of personally identifiable information and of personal information to include data in all non-digital formats and to include digital data that are protected by encryption, redaction, or another means.
- Review use of the verb "license" and correct it where necessary.
- Strike the possibility of substitute notice from the bill and require that all notices to consumers be direct notices in writing. Then convert the term "substitute notice" to "supplemental notice" and have the data collector issue the supplemental notice in addition to the direct notice.
- Require direct notice to consumers even if the data collector establishes that mis-use of the data is not reasonably possible.

Why provisions governing data brokers are unfriendly to Vermonters. (§2430, 2446, 2447)

The bill protects data brokers at the expense of consumers. Its provisions inhibit a consumer from learning about an unauthorized acquisition of the consumer's personal information and from taking timely steps to mitigate the effects of that acquisition. The bill fails to hold data brokers accountable to consumers or the State. The provisions regarding data brokers are basically worthless at protecting consumers or giving consumers information because of the paucity of information to be made available to consumers and because of the onerous conditions placed on consumers to obtain what little information will be made available to them.

Definition of a data broker

The definition of a data broker is narrow. The bill covers only a limited scope of data transactions by data brokers: selling or licensing. Those verbs do not cover all forms of transferring or sharing the data.

Registration with the Secretary of State. Annual registration with the Secretary of State leaves a gap of as much as thirteen months in a broker's first year of operation. That gap is the time between a data broker's start of operations in Vermont and the registration date of January 31. Thus there is no way for a consumer to learn of a new broker in a timely fashion. So a consumer will not know who the new data brokers are. A consumer will not know if the brokers offer any opt-out provisions until after the broker has collected the consumer's data and it is too late to opt out.

The penalty of $50 per day (capped at $10,000 per year) when a data broker fails to register with the Secretary of State, seems too low.

Too many data brokers.
Two associations that submitted letters to the House committee claim they have a combined 1700 members. I believe those members would fall under the definition of a data broker. It is unrealistic for any consumer to review each and every one of them to find out their opt-out policies and other information.

Data broker data that are not personal information. Data brokers likely will have more data on a consumer than is included in the definition of personal information. Loss of that other data will not be a data broker security breach. Giving data brokers a catch-all definition of personal information along the lines of "and any other data elements not included in personally identifiable information" is too broad.

Opt-outs. A data broker will not be required to allow a consumer to opt out of anything. The requirement will be merely to include in the registration whether and what opt-outs will be offered and all activities from which a consumer will not be able to opt-out.

The requirement for a consumer to opt-out is burdensome on a consumer. According to testimony from the National Association of Professional Background Screeners, there are over 900 entities engaged in the background screening profession. If even a small portion of them register, and only a small portion of other types of data brokers, it seems unlikely that any consumer will actually make it through the registry of all data brokers. In order to opt-out, a consumer will have to go to the internet site of the Secretary of State, research each data broker registered there, figure out what the consumer can opt out of, and then follow whatever quirky procedure each individual data broker requires.

Credentialing of data purchasers. A data broker will not be required to evaluate the credentials of purchasers of data. A data broker will need merely to state in the registration whether or not it evaluates credentials. There will be no requirement for a broker to describe the process of evaluation. That means that brokers with sketchy evaluations will get the same checkmark on the registration as brokers with in-depth evaluations. And the consumer will never know the difference, will never know which broker has which type. Also, having a data broker state whether they credential data purchasers is irrelevant if a broker that doesn't credential doesn't allow opting out.

Notice of data broker security breaches. The bill does not require data brokers to notify anyone of unauthorized acquisition of personal information. The elements of a data broker's security plan do not require notification of consumers or data collectors or attorney general or Department of Financial Regulation. So a consumer will likely never learn of a security breach involving a data broker. Instead of notices of individual breaches, a data broker will be required merely to provide to the Secretary of State an annual summary of the total number of data breaches and the total number of consumers affected. The summary will not even be a breakout by individual security data breaches.

Information security program.

A data broker will be required to "develop, implement, and maintain a comprehensive information security program". The program will need to have certain features. Yet, there will be no requirement for a data broker to reveal that plan to anyone.

The information security program will deal with personally identifiable information. Yet the definition of a data broker is that it uses personal information. This discrepancy is really confusing.

The scope of the information security program will be limited to the amount of resources available to the data broker. Some companies are set up in ways that give them few resources. This will allow a data broker with a large amount of data to evade its responsibilities through manipulation of the corporate structure or manipulation of financial arrangements.

The bill fails to describe how secure the information security program needs to be. That is because it uses undefinable words: "reasonably" (e.g., reasonably up-to-date), "appropriate", "as necessary", and others. A problem with this word is that what a data broker considers to be reasonable is likely to be far different from what a consumer thinks is reasonable. The same applies to the other words.

Correcting data. There is no mechanism under which a consumer will be able to correct information that the data broker has on the consumer. There is no ability for a consumer to request and receive a data report from a data broker, whether or not registered with the Secretary of State.

Establishing a direct relationship. The bill is not clear about what activities will establish a direct relationship with a data broker. I think the bill should be clear that the following will not establish a direct relationship.
- A consumer requesting to opt-out of a data broker's activities.
- A consumer requesting a data report or a correction to a data report.
- A consumer being required to give information to a third party in order to get the service the consumer wants.
- A data broker getting an e-mail address from a third party and then sending e-mails to that consumer.
- A consumer notifying the data broker to stop sending the e-mails.

Proposed amendments to the bill
- Expand the definition of a data broker to include all forms of transferring the personal data, beyond selling or licensing.
- Require the data brokers to register with the Secretary of State before beginning operations in Vermont. This is similar to the way that professionals need to be registered before they can begin operations.
- Amend the bill to clarify how data elements that are neither personally identifiable information nor personal information will be handled. One way is to prohibit data handlers from transfers of data elements not shown on exhibit 2.
- Require all data brokers to allow opting out. Better yet, require data brokers to have opting in as the default.
- Add a credentialing plan and its parameters to the requirements for the information security program.
- Require direct notice to consumers about unauthorized acquisitions of personal data.
- Require the data broker to provide the information security plan to the Secretary of State and to put the plan on the broker's internet site.
- Clarify whether the information security program is about personally identifiable information or personal information or both.
- Do not allow a data broker to limit the information security program based on the resources available. Rather require that the scope of the program be suitable for the amount of data involved and the damage that a breach has the potential to cause.
- Tighten up on the imprecise words, including "reasonably".
- Provide a mechanism for consumers to obtain data reports from data brokers and to correct data from the data broker, all without creating a direct relationship with the broker. The data report will include the source of the data so the consumer can also correct the data at the source.
- Clarify that opting out, correcting data, obtaining a data report, or being forced to work through a third party do not create a direct relationship between a data broker and a consumer.

Security freezes. (Secs. 3 and 4)
The bill removes fees for placing, temporarily lifting, or removing a security freeze on a credit report. I support this feature.

A consumer might want to place a security freeze when the credit reporting agency itself is the data collector that has lost control of its data. If the credit agency cannot maintain personal information securely, it seems odd that the bill expects consumers to trust that same agency to protect a unique personal identification number or password used for withdrawing or temporarily lifting a security freeze. This is requiring a consumer to trust an entity that has proven itself to be untrustworthy.

The purpose of exempting direct mail offers of credit from the freeze is not clear. It allows someone to 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, even during a freeze.

The term "pre-authorized approvals of credit" is not defined. 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.

The bill gives a credit reporting agency five business days to place the security freeze. The agency has ten business days to notify the consumer of the password to use when altering the security freeze. It is not clear whether the ten days begin with the agency receiving the request or the agency placing the freeze.

Proposed amendments to the bill.
- Remove pre-authorized approvals of credit and direct mail offers of credit from the exceptions.
- Clarify that the ten days begin when the agency receives the written notice to place the security freeze.

How consumers are kept in the dark about authorized acquisition of data. (§2430, 2435, 2446, 2447)
Consumers have little or no control over data once they have given it to a data collector. The data collector does not need to obtain permission from a consumer to disseminate the data it collected from the consumer. Data brokers will not need to obtain permission from a consumer to license or sell the data it has collected about the consumer.

Proposed amendments to the bill
- Proposed amendments on this topic are included among the other recommendations in this exhibit.

Establishing liability for data handlers. (Sec. 2)
Consumers whose data have been breached can suffer damages or identity theft as a result of the unauthorized acquisition of data. The bill does not make the data broker or the data collector that lost control of the personally identifiable information or personal information liable for any losses to the consumers whose data have been breached.

Proposed amendment to the bill
- Add provisions to make data brokers or collectors liable to consumers for damages resulting from unauthorized acquisitions of data.

Conclusion
Thank you for giving me the time to testify this morning.

You have an opportunity to make major changes to our statutes on protection of personal information. I urge you to take advantage of this opportunity by amending this bill in the ways that I have suggested in this testimony.

Sincerely,

Thomas Weiss

Exhibit 1 - data elements classified as proposed in H-764

H-764 - data brokers and consumer protection

Thomas Weiss

April 10, 2018

type of information	PII	PI	CI	SSN
name (for PII, name plus any other(s))	yes	yes	no	no
address	no	yes	no	no
name or address of immediate family or household member	no	yes	no	no
social security number	yes	yes	yes	yes
driver's license number	yes	yes	yes	yes
non-driver ID number	yes	yes	yes	yes
passport number	no	yes	yes	yes
employer taxpayer ID number	no	yes	no	yes
other government issued ID number	no	yes	no	no
biometric record	no	yes	no	no
physical characteristics or description	no	no	yes	no
date of birth	no	yes	no	no
place of birth	no	yes	no	no
mother's maiden name	no	yes	no	no
financial account number, credit card number, or debit card number that can be used without passwords, access codes, or additional identifying information	yes	no	yes: bank acct. number only	yes
financial account number, credit card number, or debit card number that requires passwords, access codes, or additional identifying information	no	no	yes	yes
financial account PIN's, passwords or other access codes	yes	no	yes	yes
credit card or debit card PIN's, passwords or other access codes	no	no	yes	yes
any other financial information	no	no	yes	no
insurance policy number	no?	no?	yes	no
signature	no	yes	yes	no
any other information that, alone or in combination, is linked or linkable to the consumer that would allow a reasonable person to identify the consumer with reasonable certainty	no	no	yes	no
credit report	no	no	no	
internet browsing history	no	no	no	
online purchases	no	no	no	
location data	no	no	no	
loyalty programs	no	no	no	
subscription information	no	no	no	

Vermont requires notice to consumers only for the unauthorized acquisition of PII (personally identifiable information) , and only in some cases. Vermont does not require notice to consumers for unauthorized acquisition of all other information.

PII - personally identifiable information (data collectors) - non-encrypted-digital only
PI - personal information (data brokers) - non-encrypted-digital only
CI - confidential information (destroyers of data records) - digital or paper
SSN - social security number protection - digital or paper

Exhibit 2 - proposed re-classification of data elements

H-764 - data brokers and consumer protection

Thomas Weiss

April 10, 2018

type of information	PII	PI
name (for PII, name plus any other(s))	yes	yes
address	no	yes
name or address of immediate family or household member	no	yes
social security number	yes	no
driver's license number	yes	no
non-driver ID number	yes	no
passport number	yes	no
employer taxpayer ID	yes	no
other government issued ID number	yes	no
biometric record	yes	no
physical characteristics or description	yes	no
date of birth	no	yes
place of birth	no	yes
mother's maiden name	no	yes
financial account number, credit card number, or debit card number that can be used without passwords, access codes, or additional identifying information	yes	no
financial account number, credit card number, or debit card number that requires passwords, access codes, or additional identifying information	yes	no
financial account PIN's, passwords or other access codes	yes	no
credit card or debit card PIN's, passwords or other access codes	yes	no
any other financial information	yes	no
insurance policy number	yes	no
signature	yes	no
any other information that, alone or in combination, is linked or linkable to the consumer that would allow a reasonable person to identify the consumer with reasonable certainty	yes	no
credit report	no	no
internet browsing history	no	no
online purchases	no	no
location data	no	no
loyalty programs	no	no
subscription information	no	no

PII - personally identifiable information - all record formats
PI - personal information - all record formats

Blocks with a grey background show changes from Exhibit 1.

Exhibit 3
Notice to consumers of unauthorized acquisitions of personally identifiable information
H.764 - data brokers and consumer protection
Thomas Weiss, April 10, 2018

References are to subsections of 9 V. S. A. 2435 unless otherwise noted.

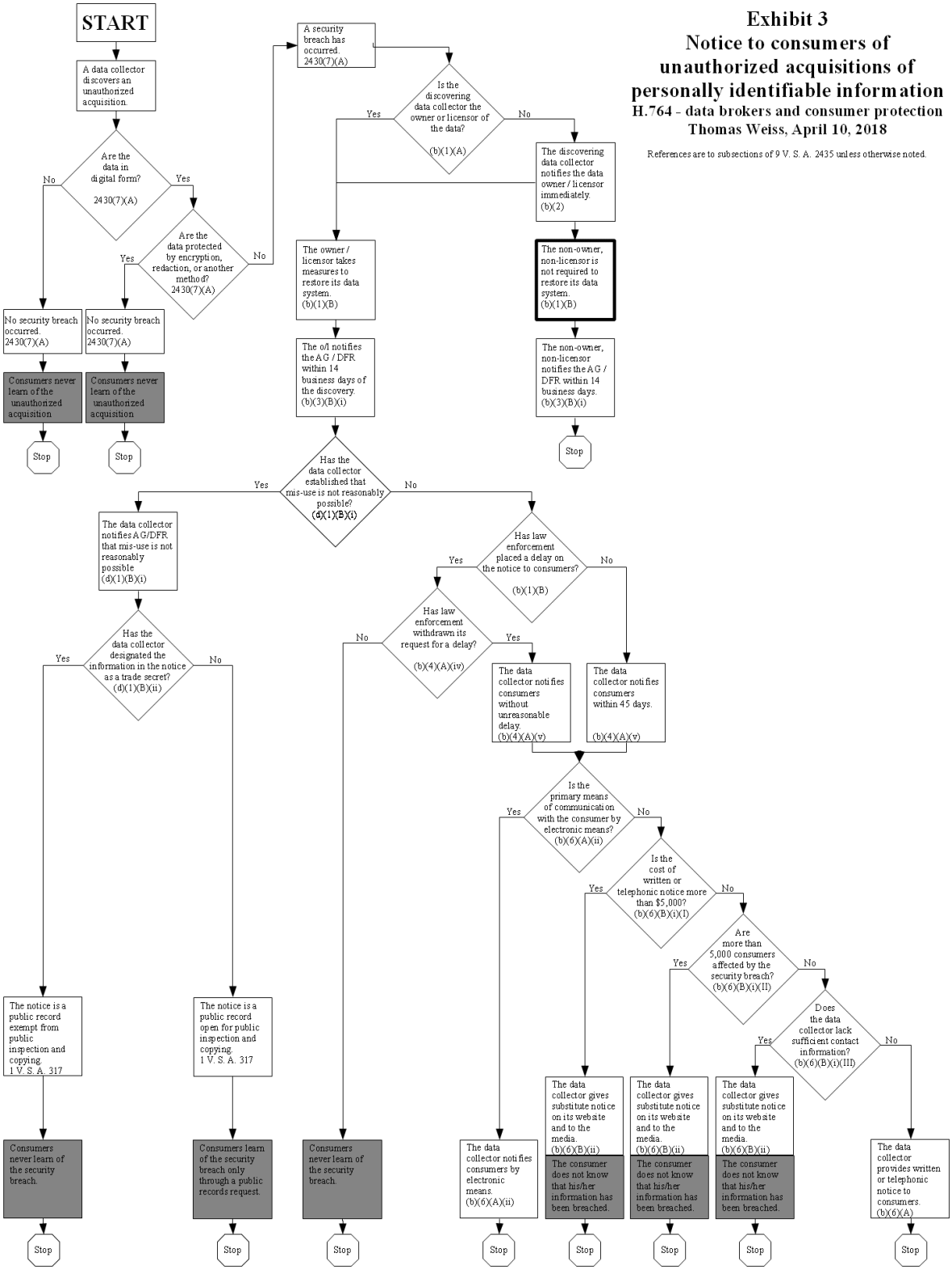

Exhibit 4 - Proposed amendments
H-764 - data brokers and consumer protection
Thomas Weiss
April 10, 2018
Part 1

The findings and intent of the bill

Proposed additional findings

- Handlers of data collect data about a consumer directly and indirectly. Many handlers of data get their data both ways. Thus, the boundaries among data collectors, data brokers, and destroyers of data records are indistinct. A given entity can be all three types of data handler simultaneously.
- Portions of the underlying statutes are weak on protection of personally identifiable information and inhibit notice to consumers. Strengthening those portions of the underlying statutes will benefit consumers.
- Some data elements are not marketable commodities. They are not to be bought and sold. These are the data elements that an individual uses to establish his or her identity. The transfer of data elements that are not marketable commodities should be defined as "data trafficking" and made a crime.
- It is specious to argue that consumers who "voluntarily" provide data have meaningful control over how the data are used.
- It is unconscionable to expect all Vermonters to have to worry about credit ratings and identity theft when as few as 5,001 have had their data stolen.
- Existing statute requires direct notice to consumers only if the cost to the data collector does not exceed $5,000. The resulting shift in cost burden to all Vermonters to investigate whether they are the ones who have been affected will far exceed $5,000.
- Data are data, no matter the form. It matters not to a consumer whether an unauthorized acquisition is on paper or through electronic files. It is now easy to convert paper documents into searchable digital forms.
- Consumers are kept in the dark about too many acquisitions of data, whether they be authorized or unauthorized. In too many instances when the acquisition is unauthorized, either the consumer never learns of the unauthorized acquisition or the consumer is not notified directly that the acquisition includes his or her data. Even when a data handler authorizes an acquisition, that is often without the knowledge or express consent of the consumer.

Proposed additional intents

- Giving the consumer more control over the use of the consumer's personal data.
- Increasing the paths leading to direct notice to consumers of unauthorized acquisitions of data.
- Declaring that the marketing of some data elements is unacceptable.
- Preventing the re-purposing of data obtained directly from a consumer

The data elements being handled and the entities that handle them

- Adopt the proposed classification of data elements as shown in exhibit 2.
- Add additional data elements to the list of personally identifiable information. Some of these elements would come from those that are determined to be exempt from disclosure as public records. (Not all of the public records exemptions, but there are some that could be added to the list.)
- Determine how to handle data elements that are not listed in Exhibit 2.
- Create the crime of data trafficking for personally identifiable information and add it to §2433.
- Change the term "personally identifiable information" to "confidential information to more accurately reflect the nature of the data elements.

Exhibit 4 - Proposed amendments

H-764 - data brokers and consumer protection

Thomas Weiss

April 10, 2018

Part 2

Relationships among categories of data handlers

- Focus on the data elements and not on the category of the entity handling the data.
- Or, explicitly state that a given entity that performs activities of more than one type of data handler must meet the requirements for all of those types of data handlers. Thus, when a given entity meets the definition of a data collector it must comply with those provisions. If it also meets the definition of a data broker it must also comply with those provisions. And if it also meets the definition of a destroyer of data records, it must also comply with those provisions.
- Review the definitions of the categories of information and of data handlers. Then make sure that their are no gaps that should be covered.

Prohibitions on data trafficking and §2433

- Expand the prohibitions to add the category of personally identifiable information where §2433 already has personal information.
- Prohibit the re-purposing of data collected directly from a consumer, unless specifically authorized by the consumer. Using privacy policies or similar requirements authorizing re-purposing of data in order to obtain a service would be prohibited. This also includes prohibiting a retailer that obtains information from a consumer in connection with an on-line purchase from selling that data or using it for any other purpose than for on-line purchases with that consumer.
- Make data trafficking a crime, which would be the buying, selling, transfer, etc. of personally identifiable information. The only legal way for a data handler to get personally identifiable information would be to receive it directly from the consumer.

Increasing the number of paths for consumer notification of unauthorized data acquisitions.

- Notify consumers immediately of an unauthorized acquisition.
- Remove the ability of law enforcement to place a hold on direct written notice to consumers.
- Require all notices to consumers to be direct notices in writing and delivered by certified mail.
- Prohibit telephonic or electronic notice unless there is some mechanism by which the consumer can be assured that the notice is legitimate and not a scam.
- Expand the definitions of personally identifiable information and of personal information to include data in all non-digital formats and to include digital data that are protected by encryption, redaction, or another means.
- Review use of the verb "license" and correct it where necessary.
- Strike the possibility of substitute notice from the bill and require that all notices to consumers be direct notices in writing. Then convert the term "substitute notice" to "supplemental notice" and have the data collector issue the supplemental notice in addition to the direct notice.
- Require direct notice to consumers even if the data collector establishes that mis-use of the data is not reasonably possible.

Exhibit 4 - Proposed amendments
H-764 - data brokers and consumer protection
Thomas Weiss
April 10, 2018
Part 3

Why provisions governing data brokers are unfriendly to Vermonters

- Expand the definition of a data broker to include all forms of transferring the personal data, beyond selling or licensing.
- Require the data brokers to register with the Secretary of State before beginning operations in Vermont. This is similar to the way that professionals need to be registered before they can begin operations.
- Amend the bill to clarify how data elements that are neither personally identifiable information nor personal information will be handled. One way is to prohibit data handlers from transfers of data elements not shown on exhibit 2.
- Require all data brokers to allow opting out. Better yet, require data brokers to have opting in as the default.
- Add a credentialing plan and its parameters to the requirements for the information security program.
- Require direct notice to consumers about unauthorized acquisitions of personal data.
- Require the data broker to provide the information security plan to the Secretary of State and to put the plan on the broker's internet site.
- Clarify whether the information security program is about personally identifiable information or personal information or both.
- Do not allow a data broker to limit the information security program based on the resources available. Rather require that the scope of the program be suitable for the amount of data involved and the damage that a breach has the potential to cause.
- Tighten up on the imprecise words, including "reasonably".
- Provide a mechanism for consumers to obtain data reports from data brokers and to correct data from the data broker, all without creating a direct relationship with the broker. The data report will include the source of the data so the consumer can also correct the data at the source.
- Clarify that opting out, correcting data, obtaining a data report, or being forced to work through a third party do not create a direct relationship between a data broker and a consumer.

Security freezes.

- Remove pre-authorized approvals of credit and direct mail offers of credit from the exceptions.
- Clarify that the ten days begin when the agency receives the written notice to place the security freeze.

How consumers are kept in the dark about authorized acquisition of data

- Proposed amendments on this topic are included among the other recommendations in this exhibit.

Establishing liability for data handlers

- Add provisions to make data brokers or collectors liable to consumers for damages resulting from unauthorized acquisitions of data.