TESTIMONY OF JORDAN ABBOTT ON BEHALF OF ACXIOM CORPORATION
January 12, 2018

My name is Jordan Abbott, I am an attorney for Acxiom, based in Little Rock, Arkansas. Thank you for the opportunity to speak with you today. It is an honor and a privilege.

By way of background, Acxiom is an information management company that is almost 50 years old and has operations around the world. Our vision is to make data valuable to everyone. Our primary business is processing our clients' data. But one of our lines of business that represents about 10% of ACXM's annual revenues involves aggregating data from various public, publicly available, and private sources, aggregating the information, enhancing it with various insights and then licensing that information to our clients who use that information, depending on the type of information we are talking about, for marketing or fraud detection and prevention purposes.

I would like to comment briefly on the proposed data broker committee bill. Before I begin I want to specially recognize the hard work that the working group, in particular, performed last year, which

ostensibly led to the proposed bill. I and our Chief Privacy Officer, Sheila Colclasure, were afforded an opportunity to testify and contribute to the working group's fact gathering process.

While we fully appreciate the Legislature's understandable and admirable goal of protecting its citizens and want to work with the Legislature, the AG, and the Commission on Financial Regulation to achieve those worthy goals, Acxiom respectfully opposes the data broker bill. Simply stated, we believe the bill is unnecessary, given current Vermont and federal laws and regulations, it unfairly distinguishes between companies based on the simple fact of licensing data to a third party. I urge the committee to not pass the bill.

Before I get into the details of the bill, I want to acknowledge that Acxiom is probably the exact type of company the proposed bill is intended to cover. While ACXM is not a consumer reporting agency under the FCRA or VSA §2480 , ACXM, nevertheless possesses certain sensitive information such as dates of birth, SSNs, and protected health information. Regardless of any definition I could possibly come up with, I doubt I could fashion one that would exempt ACXM. Such is my lot in life… However, ACXM conducts its operations in

accordance with the GLB Privacy and Safeguard Rules, the HIPAA Privacy Rule and Security Rule and where appropriate, the Payment Card Industry guidelines. We have a comprehensive information security program and client and vendor credentialing programs in place that I am comfortable in concluding already complies with the requirements in the proposed bill.

However, I believe it is important to fight for the little guy and point out that the current definition of "data broker" in the proposed bill (p. 13, 2430(3)(A)), is broadly defined to effectively include any and every business that collects information on a "prospective customer" that does not become an actual customer if they license that information to third parties. I suspect that fact is going to surprise and frustrate a lot of Vermont businesses.

The proposed bill is sweeping in its new provisions. Among other things, it purports to require an annual filing, implementation of a comprehensive information security program, and creates a "data broker" specific security breach notification program.

As I indicated at the outset, ACXM opposes the bill in general. It is unnecessary, consumers are already adequately protected by not only federal

law, but Vermont law. [Discuss underinclusive and overbroad aspects] It is troubling that Vermont seeks to expand the scope of what would trigger a security breach notification to simple things like names, addresses, and email addresses. Those things are not sensitive and do not lead to significant risk of identity theft or harm.

Moreover, certain aspects of the bill, if enacted as currently drafted, could cost millions of dollars to comply. Add to that the fact that at least two sections include a private right of action and we have the makings of substantial compliance risks.

Turning to the specific defects of the bill, I will limit my testimony to several key problematic provisions:

I would first like to focus on section 2433(b) dealing with personal information related to minors. I suspect it is intended to prohibit collection and use of data about minors for marketing use. ACXM supports that goal as I believe the Data and Marketing Association Guidelines for Ethical Business Practices do. However, the language as currently drafted is overbroad in that it creates substantial compliance obligations for risk mitigation purposes like identifying additional drivers for insurance underwriting purposes. More

fundamentally, allowing a parent to opt out of collection and use of those purposes would undermine the utility of the service and enable fraudsters to game the system which is what the service is designed to prevent. At the very least, language should be added to (b) that limits it to marketing to minors.

In addition, Section 2433(c) gives consumers a private right of action. We believe that provision should be stricken since it will generate often meritless litigation that will drain resources. But at the very least (b) must be modified if this provision were for some reason to remain.

Section 2446 requires annual registration. While not overly burdensome, my personal experience both as a former assistant attorney general and since then has been that consumers do not utilize the information and it becomes a practically meaningless annual exercise. Charities, professional fund raisers and telephone solicitors are required to register with the Arkansas AG as I believe they are in Vermont and provide far more information. Rarely did we get calls asking whether a particular entity was registered.

Section 2447 requires that a data broker implement a comprehensive information security program. As I indicated earlier, ACXM already has one as required by federal regulation and our clients.

But subsection (c)(2)(B) is incredibly problematic because it requires "personal information" to be encrypted in transit. That would require simply names and addresses to be encrypted. Laying aside any constitutional issues with Vermont imposing a clearly unreasonable burden and obligation on interstate commerce that would possibly constitute a dormant commerce clause violation, this one obligation could cost millions to comply. Why is it imperative to distinguish between data collectors and data brokers? This language needs to be modified to apply only to personally identifiable information.

Like section 2433, Subsection (d) grants consumers a private right of action. This will almost certainly generate litigation. I haven't had a chance to research Vermont case law on this issue but at the very least a consumer should have to show actual harm.

Lastly, section 2448 deals with Data Broker Security Breach Notices. It imposes an obligation on data

brokers to provide security breach notifications if something as innocuous as a name, address or email address is disclosed without authorization. At the outset, there is no legitimate justification for treating data brokers and data collectors differently particularly when data collectors have the same types of information as data brokers. Does their decision not to license information suddenly make them any less secure?

We believe a specific data broker provision is unnecessary and in any event should be limited to sensitive information as defined in “personally identifiable information”

Assuming changes are not made, the effective date needs to be extended until 2020 to give companies time to comply.

In summary, this bill is problematic not only with respect to specific provisions but overall and should not pass. I again want to express my thanks for the opportunity to provide comments and respectfully express our opposition.