TESTIMONY OF RELX / LEXISNEXIS RISK SOLUTIONS

Vermont Senate Committee on Economic Development, Housing and General Affairs
H.211 – An Act Relating to Data Brokers and Personal Information

April 15, 2026

LexisNexis Risk Solutions has been a duly registered data broker in Vermont since the inception of the State's registration requirement, and is also registered in California, Oregon, and Texas, the three other states with data broker resignation requirements.

LexisNexis Risk Solutions operates primarily in the fraud prevention, identity verification, and insurance underwriting spaces. We serve financial institutions, including banks and insurance companies, as well as government agencies throughout Vermont and the nation. We are fully supportive of comprehensive, thoughtful privacy legislation and appear before this Committee as a constructive partner in that effort.

Who We Are and How We Protect Data

LexisNexis Risk Solutions collects and uses data within a robust compliance framework that includes contractual controls, technical restrictions, credentialing, and ongoing audits. Every customer that accesses our data must pass a review process, enter into a contract certifying their permissible purpose, and comply with use restrictions that are both contractually required and technically enforced at the system level. We audit customers on the back end to ensure the data is only used as permitted.

Much of our data consists of publicly available information. We also hold datasets regulated under federal sectoral laws, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), the Driver's Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPAA), each of which is kept in separate, credentialed environments and used only for the permissible purposes those laws allow.

We also vet every data source we acquire from. If a potential source raises red flags or cannot demonstrate that it has obtained data lawfully and appropriately, we do not do business with them. Data quality is both a compliance requirement and a business imperative: inaccurate data undermines the fraud prevention services our customers rely on to protect Vermont consumers.

Vermont does not currently have an omnibus consumer privacy law in place. It is worth noting that S.71, which passed the Vermont Senate in 2025, includes a broad deletion right that would allow a consumer to request that any business, not just a data broker, delete their personal data. That broader framework is important as this committee weighs the language in H.211.

H.211 appears to be an attempt to mirror California's DELETE Act. The DELETE Act was passed after the California Consumer Privacy Act, the CCPA, was already in place. The DELETE Act was designed to address a specific technical gap in the CCPA's deletion framework as it applied to

indirect data collectors, or data brokers. It was built on top of an existing, comprehensive privacy law and designed to integrate with it.

The DELETE Act incorporates key elements of the underlying CCPA. Significantly, it cross-references and preserves the CCPA's exemptions for data regulated by federal privacy regimes, including the Fair Credit Reporting Act (FCRA), the Gramm-Leach Bliley Act (GLBA), the Driver's Privacy Protection Act (DPPA), and the Health Insurance Portability and Accountability Act (HIPPA). Additionally, all 19 states that have enacted omnibus consumer privacy laws include exemptions for these same federal laws, including those states that have both an omnibus privacy law and a data broker registration requirement (CA, OR, and TX). Those are data-level carve-outs that reflect longstanding federal consumer protection frameworks.

Concerns with H.211

1. Exemptions for Federally Regulated Data

Every one of the 19 states that has enacted a comprehensive omnibus privacy statute, including California under both the CCPA and the DELETE Act, includes exemptions for data regulated under FCRA, GLBA, DPPA, and HIPAA. These exemptions are not a loophole: they reflect a deliberate policy judgment that data already subject to detailed federal privacy, security, retention, and consumer-rights requirements should not also be subject to conflicting state deletion mandates.

H.211, as currently drafted, does not include a data-level exemption for GLBA-regulated data. This creates a direct conflict. The GLBA Safeguards Rule already mandates secure disposal of customer information within a defined timeframe. Requiring deletion on a consumer's request before that timeframe expires, or during an active fraud investigation or audit cycle, would undermine federal compliance obligations and could actually harm the consumers H.211 is intended to protect.

We respectfully request that the Committee adopt data-level exemptions for FCRA, GLBA, DPPA, and HIPAA data, consistent with the approach taken by California and the other 19 states. A data-level exemption (rather than an entity-level exemption) correctly captures the full ecosystem of service providers, including companies like LexisNexis, that handle regulated data on behalf of financial institutions.

2. The Segregation Requirement in §2446(c)(4)

Section 2446(c)(4) requires that data retained pursuant to a denial of a deletion request be "separated or segregated from data used for any other purpose." While the intent of this provision is understandable, it conflicts with the operational reality of FCRA compliance. Accurate reinvestigations, fraud flags, suppression lists, and identity verification artifacts under the FCRA require continuous cross-reference to historical records. Segregating retained data so it cannot be used for any other purpose would undermine the very accuracy and consumer-protection obligations the FCRA imposes.

We request that the Committee consider language clarifying that this segregation requirement does not apply to data that must be accessible across compliance functions to fulfill federal legal obligations.

3. Fraud Prevention and the Processor Exemption

H.211 attempts to include an exemption for data used in fraud prevention, identity theft detection, and security incident response. These are essential carve-outs. However, we wish to flag a definitional gap that could inadvertently limit their effectiveness.

The bill's processor exemption in §2446(c)(3)(vi) covers data "processed solely in the data broker's capacity as a processor to a business with which the consumer has a direct relationship." In some transactions, LexisNexis functions as a processor in this traditional sense, processing data on behalf of a specific financial institution. However, in many cases we provide our own proprietary data assets to financial institutions to support fraud prevention. In those cases, we are a controller of the data, not a processor in the strict sense, even though the functional purpose is identical: protecting consumers from fraud.

When a consumer requests deletion of data held for fraud prevention purposes, there is a risk that the deletion request itself, if processed without exception, could harm that consumer. Fraudsters increasingly attempt to erase their own records or impersonate victims in order to eliminate fraud flags. A robust deletion right that does not account for fraud prevention data could be exploited in ways that leave consumers more vulnerable, not less. A deletion mechanism is different than, for example, a credit freeze. If you have frozen your credit and want to apply for a loan, you can simply un-freeze your credit. If you have deleted (perhaps even unknowingly) data that is critical to verifying your identify and protecting against fraud, there's no way to "get that back". It's gone from the system.

This is not an argument against consumer deletion rights. It is an argument for carefully scoped exemptions that protect consumers on both ends, their privacy and their security.