Testimony of Alisoun Moore, LexisNexis Risk. Senior Director of Corporate Development for the Federal Sector

First, I would like to thank the Federal Health Policy Committee and API Task Force for the opportunity to provide comments. LexisNexis Risk provides risk mitigation services and data to many industries including healthcare. We assimilate information from over 10,000 public record sources to determine correct identities for individuals, businesses and healthcare providers. This information is used by thousands of businesses in banking, insurance, real estate, government, law enforcement, healthcare payers and providers and many others to ensure transactions can occur securely and to protect consumers. In the course of this business model we routinely offer XML and secure batch processing of customer data against our data to verify information. We do allow APIs but with strict controls and licensing for clients who need to access to either upload or download our data. We take great care with our data and our client's data providing a thorough licensing and data usage process with specific data usage agreements with our clients.

Questions for Panel 2: Consumer Technologies

1. Does your organization use APIs for apps which are available internally or to third parties? If so:

Yes, but with strict usage and access policies.

   a. Do you publish your documentation online or make it available to third party developers?

Some documentation is published online, however we work closely with clients that have special requirements for integration with their systems. All clients who wish to procure access to our data must follow our internal process for technical integration but also must conform to data usage agreements that protect their data and guide their use of our data. All clients must abide by pertinent federal and state laws such as FCRA. We are not a software firm so APIs that we develop or use are based on the client's needs and our business requirements for how we provide access to our data.

      i. How do you determine who can get access to your API?

This is based upon the clients' specific needs and what they want access to. We are a data services and analytics company and we are regulated by federal and state statutes, therefore we work closely with our clients to ensure they understand how they can use our data (i.e. permissible use) and then when agreements and licenses are signed we set up secure access using XML or, in some cases, can integrate directly into their systems to provide seamless access to our data and allow our clients secure file transfers for batch processing.

      ii. Do they need to be "certified" for privacy or security standards by your organization to use?

Yes, we do this ourselves in accordance with our privacy, security and data usage policies.

iii. Are there terms of use that include specific language for privacy and security?

Yes. We have very specific requirements for privacy and security. Our two data centers where we house our data and our clients' data are FISMA High compliant. We have developed a proprietary technology called LEXID that is an internally created unique identifier that we use for each correctly resolved identity – this masks the real identity of people and is often used by our clients who do not wish to use a Social Security Number for example.

2. Are there production deployments of these APIs/third party applications using APIs?

Yes. But again, these production deployments are for use only with clients who have completed appropriate data usage, credentialing, and licensing agreements. For instance, we receive data from property and casualty insurance companies, process that data for the industry and then allow insurance companies access to that data. This allows the property and casualty insurance industry to collectively 'share' data to prevent fraud, properly underwrite polices, and allow efficiencies such as prefilling forms to occur. This is a production system where our clients have a clear benefit but the APIs they access or we access are for a specific purpose and are, and must, be governed by data usage and licensing agreements for the protection of their data, our data and security of consumer information.

3. What are the perceived and actual privacy and security concerns or barriers to the adoption of APIs?

a. How can these risks be mitigated/how are you addressing this?

Like any technology, if the APIs are not developed or governed with strict security controls and data usage policies security and privacy will be compromised. This can lead to data breaches and all developers, companies, the government and consumers should be wary of poorly designed APIs and a lack of governing documentation. LexisNexis understands this and has a strict process on the development of our internal APIs and data usage and licensing agreements for access to our products and services. Likewise if our clients want specific integration of our system to theirs we require the same from them and we document our agreements. We have built entire businesses on this model. Trust that we will handle our clients' data with great care is built upon the foundation of a secure infrastructure, and strict adherence to our data usage agreements. This also, of course, allows us to abide by all applicable laws and regulations.

4. How to improve consumer experience with the third party apps using the APIs?

Assuming you have done what I have indicated thus far in my testimony, the application must be easy to use and secure. It must be seamless and useful. Use of focus groups to test the apps and development of intuitive user interfaces are key to ensure this occurs. For instance, In our law enforcement and insurance businesses we offer seamless interfaces and sub-second response times with many drill down capabilities for additional information. This allows for very quick access to actionable information for our clients and helps them with fulfilling their

missions. We also offer pre-fil capabilities to ensure end users do not have to re-key information into their own systems.

Are there third party certifying authorities in non-healthcare industry that we can leverage?

I am not aware of any.