What's on the Horizon in Washington, DC and in the States – A Legislative Update
By implementing baseline security standards, Congress is seeking to address the increasing use of personal information by organizations and the risk that arises from data breaches.

Introduction
Over the past few years we have seen an increased focus from Capitol Hill on the use of consumer information. From Data Security laws to debates about online privacy, policy makers are attempting to find the right balance of encouraging safe business practices and innovation while protecting consumer’s personal information.

This White Paper is a brief overview of the topics at the forefront of the information privacy debate and addresses some of the key issues in the handling of consumer data. The issues covered below are likely to be topics that are debated for an extended period of time; however, we can expect to see continued pressure from consumer and privacy advocates to drive the development of improved business practices and additional regulation.

For now, these issues are important to be aware of as organizations continue to make critical and strategic business decisions based on their ability to use consumer information.

Cyber Security
Over the past several months, two Senate committees have examined and approved legislation to provide the federal government more oversight over critical network infrastructure. However, combined with other data security proposals, there are concerns over the degree of government’s role in regulating the security of private networks.

The Senate Homeland Security and Governmental Affairs Committee and the Commerce Committee have approved separate bills intended to strengthen and coordinate the security of federal civilian and critical infrastructure networks. The goals of each proposal are similar, but the locations of the new oversight responsibilities are different. The Homeland Security Committee would place the operational center for civilian cyber security within the Department of Homeland Security (DHS) and establish a permanent Office of Cyberspace Policy within the White House. The second proposal by the Commerce Committee would place the cybersecurity office within the White House. What are similar between the two proposals are new requirements on private organizations. The initiative would propose a baseline set of security requirements and require private-sector operators of critical infrastructure to report major breaches. Senate leadership is working to combine the two pieces of legislation and its goal is to have a final proposal considered by the full Senate during a possible lame duck session. It is uncertain whether this can be achieved.

Data Security
Data security legislation is gaining attention in Congress that would require the Federal Trade Commission to require each company or person engaged in interstate commerce that owns or possesses certain electronic data to establish security policies and procedures. There has been a long-running push in Congress for a federal data breach standard intended to preempt the number of state laws that currently govern security and notification requirements, and business general supports such an effort. Currently, 46 states, as well as the District of Columbia, Puerto Rico and the Virgin Islands have data breach laws on their books. By implementing baseline security standards, Congress is seeking to address...
the increasing use of personal information by organizations and the risk that arises from data breaches. The House of Representatives has already approved a bill, H.R. 2221 (Rush). The most recent federal effort to preempt state laws on the subject (S. 3782) was introduced by Sen. Mark Pryor (D Ark), chairman of the Subcommittee on Consumer Protection, Product Safety, and Insurance, and co-sponsored by Sen. John D. Rockefeller IV (D W.Va.), Chairman of the Senate Commerce Committee. There is concern, however, that both the Rush and Pryor legislative proposals would create obligations beyond what currently exists in state law, including the expansion of what is considered “personal information.”

Online Privacy
From legislators to regulators to consumer and privacy advocates, the public policy debate about the future of online privacy is heating up. Over the past year, a number of new proposals and hearings have taken place to examine the collection and use of consumer information. Policy makers are attempting to find the right balance of encouraging online innovation while protecting personal information.

In the meantime, Congress has already begun to draft legislation. After several years of discussing privacy legislation, two proposals were elevated earlier this year. House Energy and Commerce Subcommittee Chairman Rick Boucher (D-VA) released the draft “discussion draft” that would require Websites to provide enhanced notice about how they use consumer information and obtain a user’s consent before collecting sensitive information or sharing data about a consumer with some third parties. The draft would also require companies to “conspicuously” display a clearly written, understandable privacy policy that explains how information about individuals is collected and used. Another Subcommittee Chairman of the Energy and Commerce Committee, Rep. Bobby Rush (D-III.) introduced H.R. 5777, called the “Best Practices Act.” The complexity of both proposals is making many in the industry cautious about how Congress might move forward. Congressional hearings have been held and more are expected during the Fall, although it is very unlikely that legislation will be enacted this year.

FTC Report on Privacy Roundtables
Earlier this year, the Federal Trade Commission (FTC) held a series of day-long roundtable meetings to examine the privacy challenges created by new technology. Part of the discussion focused on the business practices of data brokers, particularly how consumer information is used. The roundtable meetings covered a wide array of topics, from social networking to online advertising and mobile marketing, and brought together representatives from business, academics and consumer groups. The FTC is now working on a report that will outline the issues and concerns raised during the series and is expected to make a number of recommendations.

Negative-option Marketing
The use of negative option marketing is becoming a dominant practice on the internet, allowing consumers to try out new products and services. Still, state attorney generals and the Federal Trade Commission (FTC) have begun to examine the practice as some companies using deceptive practices have increased the number of consumer complaints to regulators. Legislation has been proposed in a number of states, as well as in Congress,
that would require companies to provide new disclosures in advertising and send notices to consumers prior to billing. The FTC and attorney generals have a number of tools to fight deceptive practices but have been exploring whether existing regulation is sufficient in this area or new laws are needed to protect consumers. For companies using negative-option marketing, following industry best practices will continue to be important.

Consumer Financial Protection Bureau
After months of deliberation, Congress approved sweeping reforms for the financial services industry. While the legislation has been signed by President Obama, it will be some time before the industry actually feels or understands the full impact of the new law. The measure takes a broad brush to changes in the industry, leaving the details up to the financial regulators, who will be tasked with writing the impending rules over the next several years.

The new law, called the Dodd-Frank Act, will change the way many large and small financial institutions operate, likely placing downward pressure on the availability of consumer credit. At the center of the measure is the creation of a new regulatory body, called the Bureau of Consumer Financial Protection (CFPB). The CFPB will have the authority to write consumer protection rules for banks and nonbank financial firms offering consumer financial services or products, with the ability to place restrictions on the type of financial products and services offered to consumers. With respect to consumer protection and privacy, it is expected that the new bureau will focus on meaningful notices that are easy to read and understand. It is expected that the CFPB will first address lending products and practices in the mortgage industry. The bill also requires the Federal Reserve Board to write new rules limiting the interchange fees for debit cards. The provision allows merchants to offer discounts for using a particular type of payment and would prohibit discrimination based upon a network or issuer. In considering an appropriate interchange fee, the Federal Reserve may take into account the cost of fraud but is not required to do so.

Specific to large financial institutions, the Dodd-Frank Act imposes a number of new compliance requirements. The law places stricter risk-based capital requirements on financial institutions, with a maximum 15-to-1 leverage ratio for systemically important firms. Bank holding companies also have new leverage requirements to put them on par with banks, with exemptions for bank holding companies that have consolidated assets of less than $15 billion.

Conclusion
In summary, there are a great number of issues being discussed among policy makers in Washington, DC that will impact the future of privacy. Moving forward, it will be important for organizations to monitor legislative developments as Congress considers reforms of how companies handle consumer data and proposes restrictions on its use. Now, more than ever, organizations should be prepared to engage in industry best practices in order to protect themselves from increased regulatory oversight.

To learn more about data breach resolution, visit www.Experian.com/DataBreach, or contact Experian® at DataBreachInfo@Experian.com or 1 866 751 1323.