Comprehensive Data Security Legislation Passed
By Three House Committees; Senate Banking Committee Members Introduce New Bill

In March, and again in late May, legislative activity on federal data security legislation readied itself for possible action on the Floor of the House of Representatives. On March 16, the House Financial Services Committee passed its bill, the Financial Data Protection Act of 2006 (H.R. 3997), by a bipartisan recorded vote of 48-17.\(^1\) Two weeks later, on March 29, the House Energy and Commerce Committee unanimously voted 41-0 to report its version, the Data Accountability and Trust Act (H.R. 4127), also known as “DATA.”\(^2\) Finally, on May 25, the House Judiciary Committee amended and ordered to be reported by voice vote its bill, the Cyber-Security Enhancement and Consumer Data protection Act of 2006 (H.R. 5318).\(^3\)

The Senate also saw the introduction, on June 26, of its latest comprehensive data security bill, the Data Security Act of 2006 (S. 3568).\(^4\) The bill was referred to the Senate Banking Committee, and it is expected that the Committee will soon initiate a legislative hearing on S. 3568 in preparation for an eventual markup. If S. 3568 is reported to the floor, it will mark the fourth major data security bill reported to the Senate floor in the 109th Congress, joining S. 1408 reported by the Senate Commerce Committee nearly one year ago, and S. 1789 and S. 1326 reported by the Senate Judiciary Committee in the Fall of 2005.

A report on the Energy and Commerce Committee and Financial Services Committee sessions in which the committees considered their own text is provided below in section one, followed by a chart in section two comparing the key provisions of the bills, as originally reported (before sequential referrals to other committees). A report on the House Judiciary Committee follows in the third section, including a discussion of the

---

1 H.R. 3997, the Financial Data Protection Act, is sponsored by Rep. Steven LaTourette (R-OH) and cosponsored by Reps. Darlene Hooley (D-OR), Mike Castle (R-DE), Deborah Pryce (R-OH) and Dennis Moore (D-KS).

2 H.R. 4127, the Data Accountability and Trust Act or “DATA,” is sponsored by Rep. Cliff Stearns (R-FL) and cosponsored by Reps. Deborah Pryce (R-OH), Fred Upton (R-MI), George Radanovich (R-CA), Charles Bass (R-NH), Mary Bono (R-CA), Mike Ferguson (R-NJ) and Marsha Blackburn (R-TN). All but Rep. Pryce are members of the House Energy and Commerce Committee.

3 Additionally, each Committee was granted sequential referrals to consider the reported legislation of one other House Committee and did so on May 24 and 25, as more fully discussed in Section 3 below.

4 S. 3568, the Data Security Act of 2006, is sponsored by Sen. Bob Bennett (R-UT) and Sen. Tom Carper (D-DE). Both are members of the Senate Banking Committee.
sequential referrals. Finally, an analysis of the newly introduced S. 3568 is presented in the fourth section.

**Section One – Committee Markup Reports**

**1. House Financial Services Committee Markup of H.R. 3997**

When the House Financial Services Committee’s bill, H.R. 3997, was considered in March, the following amendments were offered and ultimately approved, by voice vote:

- A Manager’s Amendment offered by Rep. Mike Castle (R-DE) to make technical corrections to the bill and to add a credit freeze (patterned after the Vermont state statute) for consumers who have been a victim of identity theft.
- A Rep. Steven LaTourette (R-OH) amendment to adjust the “trigger” and create a uniform standard for data security regulations.
- A Rep. Rubén Hinojosa (D-TX) amendment to require the General Accountability Office to conduct a study to determine a system that would provide notices of data breaches to consumers in languages other than English.
- A Rep. Barbara Lee (D-CA) amendment to require the Federal Trade Commission (“FTC”) to coordinate with other government entities to create a publicly available list of data security breaches that have triggered a notice to consumers within a twelve month period.
- A Rep. Joe Baca (D-CA) amendment to require the FTC to work with international, national, and state law enforcement officers and agencies to provide voluntarily supplied information on the race and ethnicity of consumers who have been victims of data theft and account fraud.
- A Rep. Edward R. Royce (R-CA) and Rep. Paul E. Kanjorski (D-PA) amendment to update the Credit Repair Organization Act (CROA) to narrow the definition of a credit repair organization by establishing a narrow activity-based exception for credit monitoring activities. The FTC has indicated that it sees little basis to subject the sale of credit monitoring and similar educational products and services to CROA’s specific prohibitions and requirements, which were intended to rein in fraudulent credit repair.

**2. House Energy and Commerce Committee Markup of H.R. 4127**

Shortly thereafter, on March 29, 2006, the House Energy and Commerce Committee passed H.R. 4127, by a unanimous vote of 41 to 0. Virtually all of the comments by committee members were supportive of the legislation, although some Democrats argued that more should be done to expand the provisions of the bill relating to potential
identity theft. For example, Rep. Sherrod Brown (D-OH) expressed the view that the bill should also contain credit freeze language, but declined to offer an amendment. Chairman Barton responded by noting that the Committee Report that will accompany the bill will address some of those issues. Of particular note, Rep. Anna Eshoo (D-CA) was assured by the Chairman that the report would discuss her views on encryption and the value of other technologies that render data “unusable.” Rep. Eshoo argued during the markup that there are ways other than encryption to protect information and render it unusable, and that the bill should be both technology- and method-neutral.

The Committee considered four amendments to the Manager’s Amendment, as follows:

- Rep. Ed Markey’s (D-MA) amendment on Social Security numbers (SSN)—offered and withdrawn;
- Rep. Ed Markey’s (D-MA) amendment on off-shoring of personal information—offered and defeated by voice vote, and subsequently defeated by show of hands 9-17;
- Rep. Marsha Blackburn’s (R-TN) amendment on substitute notice for small business – offered and withdrawn; and
- Rep. Vito Fossella’s (R-NY) amendment on Gramm-Leach-Bliley Act (GLB) exemption – offered and withdrawn.

After consideration of the these amendments, the Manager's Amendment, as noted above, was adopted by voice vote, and the bill as amended was approved by unanimous roll call vote of 41-0. The bill, as passed by the Committee, covers “each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information” [section 2(a)(1), emphasis added]. It excludes from coverage those entities whom the FTC “determine[s]” are “required under any other federal law to maintain standards and safeguards for information security and protection of personal information that provide equal or greater protection” than that called for in the bill [sec. 2(a)(3)].
## Section Two – Comparison of Provisions of H.R. 3997 and H.R. 4127

<table>
<thead>
<tr>
<th>PROVISION</th>
<th>H.R. 3997</th>
<th>H.R. 4127</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. General Duties</td>
<td>“[R]easonable policies and procedures” aimed at protecting “sensitive financial personal information … against any loss, unauthorized access, or misuse that is reasonably likely to result in harm or inconvenience” [proposed section 630(a)(2)].</td>
<td>“[R]equire[s] each person engaged in interstate commerce that owns or possesses data in electronic form containing personal information, or contracts to have any third party entity maintain such data for such person, to establish and implement policies and procedures regarding information security practices for the treatment and protection of personal information”[sec. 2(a)].</td>
<td>H.R. 4127 applies only to electronic data; H.R. 3997 covers paper as well.</td>
</tr>
<tr>
<td>2. Personal Information</td>
<td>“[S]ensitive financial personal information” that is either “sensitive financial account information” or “sensitive financial identity information” or both.</td>
<td>“Personal information” is an individual’s first name or initial and last name, address, or phone number, in combination with any one or more of the following: SSN, driver’s license number, or other state ID number, or financial account number, credit or debit card number and any required security code, access code or password necessary to permit access to an individual’s financial account [sec. 5(7)(A)]. FTC may modify the definition of “personal information” through a rulemaking [sec. 5(7)(B)].</td>
<td>H.R. 3997 is more cumbersome but does differentiate between credit fraud and identity theft, which H.R. 4127 does not. H.R. 4127 permits FTC to modify by rule the definition of “personal information” without congressional action, creating legal uncertainty.</td>
</tr>
<tr>
<td>3. Data Breach</td>
<td>“[A]ny loss, unauthorized acquisition, or misuse of sensitive financial personal information handled by a consumer reporter that could be misused to commit financial fraud (such as identity theft or fraudulent transactions made on financial accounts) in a manner causing harm or inconvenience to a consumer” [sec. 630(m)(1)].</td>
<td>“[T]he unauthorized acquisition of data in electronic form containing personal information” [sec. 5(1)].</td>
<td>Effect of the definitions is dramatically affected by other terms and provisions in the legislation.</td>
</tr>
<tr>
<td>PROVISION</td>
<td>H.R. 3997</td>
<td>H.R. 4127</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4. Breach Notification</td>
<td>Notification if, after investigation by the consumer reporter, a breach is reasonably likely to have occurred or is “unavoidable” and the data “is reasonably likely to have been or to be misused in a manner causing harm or inconvenience” to the consumer or to “commit identity theft” or “make fraudulent transactions” [sec. 630(f)(1)].</td>
<td>Notification under this bill occurs when the applicable data is “acquired” by an “unauthorized person” following a breach. Creates a blanket exemption notification coverage if “there is no reasonable risk of identity theft, fraud, or other unlawful conduct” [sec. 3(f)]. Moreover, the bill creates a presumption that no such risk exists if the data is encrypted [sec. 3(f)(2)(A)]. Both “triggers” are complicated as they encompass other terms and provisions in the bills. H.R. 3997 requires a cumbersome investigation, but H.R. 4127 has a lower threshold for notice. “Identity theft” is broadly defined and the effect is the same as H.R. 3997.</td>
<td></td>
</tr>
<tr>
<td>5. Encryption</td>
<td>Allows covered entities to “consider” whether the potentially breached information is “unusable,” and thereby not subject to a notification obligation, if it is encrypted, redacted, requires technology that is not generally available, or has otherwise been rendered unreadable” [sec. 630(b)(3)(B)].</td>
<td>Rebuttable presumption that there is “no reasonable risk of identity theft, fraud or other unlawful conduct” if the electronic data subject to a possible breach have been encrypted [sec. 3(f)(2)(A)]. The bill requires the FTC within nine months to identify other means by which data may be effectively rendered “unreadable or indecipherable” and establish a presumption that applies to that methodology also [sec. 3(f)(2)(B)]. H.R. 3997 has more flexibility in recognizing additional methods of protecting and securing data. Presumption in H.R. 4127 is preferred.</td>
<td></td>
</tr>
<tr>
<td>6. Additional Requirements</td>
<td>Entities issuing notifications must offer a nationwide credit monitoring service to each consumer (free), for at least six months (at request of consumer within 90 days of being notified of the security breach) [sec. 630(h)].</td>
<td>Entities notifying consumers of security breaches must provide, at no cost to each notified individual, quarterly consumer credit reports for a period of two years [sec. 3(e)]. The FTC must be notified in the event of any breach of security [sec. 3(a)(2)]. Comparable.</td>
<td></td>
</tr>
<tr>
<td>PROVISION</td>
<td>H.R. 3997</td>
<td>H.R. 4127</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>7. Preemption</td>
<td>Preempts all state laws &quot;with respect to&quot; their efforts to regulate the protection and security or confidentiality of information maintained on consumers, safeguarding information from misuse or potential misuse; investigating or providing notices of a breach of security; mitigating any harm or loss due to the breach of security; or involving credit freezes [sec. 630(n)(1)].</td>
<td>“[S]upersedes” state laws that “expressly” require information security practices and notification following unauthorized acquisition of data in electronic form, so long as they are “similar to” those outlined in the bill [sec. 6(A)]. The bill expressly states, however, that it does not preempt state laws dealing with trespass, contracts, or tort to the extent those acts relate to fraud [sec. 6(c)].</td>
<td>H.R. 3997 is preferable – H.R. 4127 potentially opens the door to actions through state tort law and other laws.</td>
</tr>
<tr>
<td>8. Enforcement</td>
<td>Exclusively with the federal functional regulators, including the FTC, for the covered entities [sec. 630(k)(1) and sec. 630(l)]. Insurance, historically regulated at the state level, is treated differently [sec. 630(l)(1)(G)].</td>
<td>Federal enforcement rests exclusively with the FTC [sec. 4(a)]. State attorneys general, as well as undefined state “officials or agencies,” may bring civil actions on behalf of the residents of the state to, among other things, obtain civil penalties, capped at $5 million (caps are also indexed for inflation) [sec. 4(b) and sec. 4(b)(2)].</td>
<td>H.R. 3997 is preferable – H.R. 4127 permits state AG action (as well as other undefined officials or agencies).</td>
</tr>
<tr>
<td>9. Safe Harbors</td>
<td>“[S]upersedes” the security guidelines promulgated pursuant to section 501(b) of GLB [sec. 630(j)(1)], for both depository and non-depository institutions, and it attempts to harmonize the regulatory guidance issued by functional regulators.</td>
<td>Authorizes the FTC to determine compliance for entities outside its traditional jurisdiction, based on whether other federal laws regarding personal information security protection standards and safeguards are “equal or greater” than those required under this bill [sec. 2(a)(3)].</td>
<td>H.R. 4127 is problematic due to broad new FTC authority that is outside its expertise.</td>
</tr>
<tr>
<td>PROVISION</td>
<td>H.R. 3997</td>
<td>H.R. 4127</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10. Access and Correction</td>
<td>No provision.</td>
<td>Information brokers are obligated, at least once a year, to provide any individual who requests it, free of charge, access to “any personal information [it maintains] regarding” such individual, as well as “any” information it maintains that specifically identifies that individual (other than name or address) [sec. 2(c)(3)(B)(i)]. If any of the information is disputed, via written request, the information broker must either 1) correct the inaccuracy or, in the case of “public record” information, 2) inform the individual of its source, or, for non-public information, 3) note the disputed nature of the information, including the individual’s written statement, and “take reasonable steps to verify” the information [sec. 2(c)(3)(B)(ii)]. Access and correction is unrelated to the core issue of data security. The language in H.R. 4127 may have the effect of reducing the reliability of information commercial, non-profit and government agencies use to verify identities, enforce contracts and detect and prevent financial fraud, including identity theft.</td>
<td></td>
</tr>
<tr>
<td>11. Additional FTC Authority</td>
<td>No provision.</td>
<td>See earlier description of “personal information” (#2 above). See commentary in #11 below.</td>
<td></td>
</tr>
<tr>
<td>12. Destruction of Paper Documents</td>
<td>No provision.</td>
<td>FTC may, if feasible, set a standard for destruction of paper and other non-electronic data containing personal information if: improper disposal leads to identity theft, fraud or unlawful conduct; standards would be effective in preventing identity theft, fraud or unlawful conduct; the benefit outweighs the cost; and compliance would be “practicable” [sec. 2(b)]. This provision could potentially be burdensome for a wide variety of businesses if FTC does not recognize differences in business models and practices.</td>
<td></td>
</tr>
<tr>
<td>13. Credit Freeze</td>
<td>Permits consumers who have been victims of identify theft to place (at no cost to them) a credit freeze on a consumer reporting agency file if they make the request in writing, submit an identify theft report to the consumer reporting agency, and provide proper identification to the consumer reporting agency. No provision. Credit freeze is not germane to the issue of data security. However, this provision does recognize that the ability to request a credit freeze should be tied to actual risk to the account holder.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PROVISION</td>
<td>H.R. 3997</td>
<td>H.R. 4127</td>
<td>COMMENTS</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>14. Public Information</td>
<td>No provision dealing specifically with “public information.” See earlier description of “personal information” (#2).</td>
<td>The “access and correction” provisions (see discussion, #10, above) distinguish between what is “public record” and what is “non-public record,” and the bill defines public record information as information about an individual that has been “obtained originally” from federal, state or local government entity that are available “for public inspection” [sec. 5(9)].</td>
<td>The approach in H.R. 4127 is extremely convoluted and information that is clearly within the public domain may nevertheless not be “public records” under this provision.</td>
</tr>
<tr>
<td>15. Property Right</td>
<td>Excludes any language that might, if so interpreted, give rise to the establishment of a new property right in factual information.</td>
<td>Contains no fewer than six characterizations of the ownership of data as belonging to the consumer [see, e.g., sec. 2(c)(3)(B)(i)(l), sec. 2(c)(3)(B)(ii), sec. 3(a)(1), sec. 3(d)(2)(C)(i), sec. 3(e), and sec. 5(7)(A)(ii)].</td>
<td>H.R. 4127’s language has significant potential for use in changing legal interpretation of the First Amendment’s application to factual information.</td>
</tr>
</tbody>
</table>

Section Three – House Judiciary Committee Action (H.R. 5318)

Following the adoption of H.R. 4127 (House Energy and Commerce Committee) and H.R. 3997 (House Financial Services Committee), both Committees sought sequential jurisdiction to review each other’s bill, claiming that each one contained items and language within the jurisdiction of their respective committees. The House Judiciary Committee, which had been relatively inactive, sought sequential referral of both bills for the same reason. The House Parliamentarian granted the Energy and Commerce Committee a referral until June 2, 2006, to review H.R. 3997, and the House Financial Services Committee was granted a similar referral to review H.R. 4127, with the same deadline. The House Judiciary Committee, however, was only granted permission to review H.R. 4127 (also until June 2). Additionally, the House Judiciary Committee introduced and reported, on May 25, its own bill on the subject (H.R. 5318).

The House Judiciary Committee bill, H.R. 5318, the Cyber-Security Enhancement and Consumer Data protection Act of 2006, is much narrower than either H.R. 4127 or H.R. 3997. Its focus is exclusively on criminal conduct, and its coverage trigger is a high one. For example, its provisions obligate the owner or custodian of electronic data to notify the Secret Service and the FBI within 14 days of “discovery of the breach” [section 7(b)(1)]. Failure to do so will subject that person to criminal penalties that include fines and/or imprisonment for up to five years. To be subject to such criminal prosecution, however, one must (1) own or possess electronic data, (2) have knowledge of a “major security breach” (defined below),

---

5 H.R. 5318, the Cyber-Security Enhancement and Consumer Data protection Act of 2006, is sponsored by Chairman James Sensenbrenner (R-WI), along with Reps. Howard Coble (R-NC), Lamar Smith (R-TX), Tom Feeney (R-FL), Adam Schiff (D-CA) and Deborah Pryce (R-OH). Ms. Pryce, who chairs the Republican Conference, is the only member to co-sponsor all three House committee security breach bills.
(3) “knowingly” fail to provide notice of the breach to the Secret Service and the FBI, and
(4) do so “with the intent” to “prevent, obstruct, or impede” a lawful investigation [proposed
section 1039(a), in section 7(a) of the bill].

A “major breach” is defined as a security breach that involves the acquisition of personal
information pertaining to 10,000 or more individuals and “causes a significant risk of identity
theft” [proposed section 1039(b)(1)(A)]. The bill goes on to then define “significant risk of
identity theft” as a risk that a “reasonable person” would conclude establishes a greater
probability than not that identity theft has occurred or will occur as a result of the breach
[proposed section 1039(b)(2)].

These standards are more in keeping with the views of the Chairman of the Federal Trade
Commission, Deborah Majoras, in her public comments on the subject. Additionally, as
narrowly tailored, they do not raise the same concerns as the proposed criminal provision
for “concealment of a breach” in S. 1789, reported by the Senate Judiciary Committee in
November of 2005.

**Exercise of Sequential Jurisdiction by All Three Committees**

As noted previously, all three committees were granted sequential referrals to review
the other committees’ legislation until June 2. The House Financial Services Committee
and House Energy and Commerce Committee received sequential jurisdiction over each
other’s bill, and when they marked up those bills on May 24th, just before the Memorial
Day recess, they chose merely to substitute the text of their respective bills.6 The House
Judiciary Committee chose to report H.R. 4127 in nearly the same form in which it was
referred, amending it only slightly – in light of the recent security breach at the Veterans
Administration – to require federal agencies to provide consumer notices in the event
of certain breaches of data in the possession of those agencies. Additionally, Chairman
Sensenbrenner noted, by way of explaining the Committee’s limited action at the
markup, that, while he had severe reservations about portions of H.R. 4127, the House
Leadership wished to move some consensus bill to the House Floor and he did not want
to delay it. He also added that he would become more actively engaged as the bill neared
Floor consideration.

In the brief time since, there have been several informal meetings of the House leadership
staff and representatives of the jurisdictional committees, and the specific dates previously
reserved for possible House Floor action have been set aside while the staff continues
to negotiate. Chairman Barton has made it clear that he believes his Committee’s bill,
H.R. 4127, is the “most bipartisan” bill under consideration and therefore should take the
form of the underlying text for purposes of Floor consideration. Chairman Oxley, whose
bill also garnered substantial Democratic support, takes a contrary view.

---

6 The end result of these committee actions was to simply effect a bill number swap between H.R. 4127 and H.R. 3997, as the
text of the former (as originally reported from Committee) now contains the text of the latter, and vice-versa. To avoid confusion,
however, this memo analyzes the text produced by the Energy and Commerce Committee as if it were still numbered H.R. 4127,
and the text of the Financial Services Committee as if it were still numbered H.R. 3997.
Whether or when a House consensus bill will emerge for Floor consideration is unclear at this juncture, but it is still possible it could occur before the next congressional recess in August. What does seem apparent, however, is that if a large breach of personally sensitive data were to occur in the private sector, as it did recently involving Veterans Administration data, a political stampede would likely take place, with potentially disastrous results for proponents of a balanced and predictable preemptive national standard for data security and consumer notification.

Section Four – New Senate Banking Legislation (S. 3568)

On June 26, Sen. Bob Bennett (R-UT) and Sen. Tom Carper (D-DE), both of whom are members of the Senate Banking Committee, introduced the “Data Security Act of 2006” (S. 3568), which was then referred, as expected, to the Senate Banking Committee for consideration. It most likely represents the last in a series of bills considered by three key Senate Committees, following the reporting of bills by the Senate Commerce Committee (S. 1408) and the Senate Judiciary Committee (S. 1789 and S. 1326) last year. It is expected that S. 3568 will be brought before the Senate Banking Committee in a full committee legislative hearing before the August recess.

The legislation is narrowly targeted at addressing the data security issues (and not unrelated issues) within the jurisdiction of the Senate Banking Committee, perhaps reflecting concerns expressed by Senate Banking Committee Chairman, Richard Shelby (R-AL) about the breadth of the bills reported by the Senate Commerce Committee and Senate Judiciary Committee that arguably strayed beyond the boundaries of their respective committees’ jurisdictions in certain areas.

The provisions of the bill therefore cover entities covered by the FCRA or engaged in “financial activities,” a “financial institution,” or that otherwise “maintains or communicates sensitive account information or sensitive personal information.” Like H.R. 3997 in the House, S. 3568 focuses on the “usability” of information. Specifically, a “breach” is defined along the lines of the California statute, in that it applies whenever “sensitive account information” or “sensitive personal information” has been acquired. In turn, however, a breach is further narrowed to apply to data that is usable to commit identity theft or to make fraudulent transactions on financial accounts. The bill further notes that data is deemed unusable if it is “encrypted, redacted, altered, edited, or [in] coded form.”

“Sensitive account information” is defined as a financial account number (including a credit or debit card), in combination with a security or access code, while the term “sensitive personal information” means the first and last name, address or telephone number of a consumer, in combination with any one or more of the following: social security number, driver’s license, or taxpayer ID number. “Sensitive personal information,” however, does not include publicly available information that is “lawfully” made available to the public via government records or media distribution.
S. 3568, again like H.R. 3997, ties the obligation to provide security – and therefore notification – to whether the unauthorized use of such information is “reasonably likely to result in substantial harm or inconvenience” to the consumer “to whom the information relates.” By the use of this latter reference, the bill takes pains to eliminate the possibility of a property right emerging from an interpretation of its provisions. The bill takes the phrase “substantial harm or inconvenience,” found in GLB, and defines it to mean “material financial loss,” or criminal or civil penalties imposed upon a consumer as a result of the unauthorized use of this information, or the need for the consumer to expend “significant time and effort” to correct erroneous information resulting from its use. Importantly, the bill also notes that “substantial harm or inconvenience” does not include “harm or inconvenience that does not result from identity theft or account fraud.” This latter proviso is critical because it means that the security and notification obligations that flow from a breach of covered data do not apply unless it is reasonably likely that identity theft or account fraud will result.

S. 3568 creates security and notification obligations for covered entities, and it ties those requirements, as noted previously, to identity theft or account fraud, rather than the wholesale obligation that currently applies to entities across the board in California. Like GLB, it also allows the obligatory procedures and policies designed to carry out those obligations to take into consideration the “size and complexity” of the covered entity, the “nature and scope” of the activities of that entity, and the sensitivity of the data to be protected. In the event of the discovery of a breach, the bill requires the covered entity to conduct an investigation and notify a list of entities, including law enforcement agencies, in a prioritized order, before notification is required to be made to consumers. Additionally, a delay in consumer notification may occur if the noticed law enforcement agency makes a written request to delay such notice. Finally, the bill provides a carve-out for entities already in compliance with GLB.

Enforcement under the legislation is administrative only, imposed by functional regulators, including, as appropriate, the FTC for entities not otherwise subject to functional regulation. Like H.R. 3997, insurance companies are to be regulated by state insurance authorities. Importantly, S. 3568 also specifically bars any private right of action, including class actions, for violations of the bill’s provisions, and precludes the initiation of any civil or criminal action in “any State court or under State law.”

Lastly, the preemption provisions of S. 3568 are quite strong. No laws or “requirement[s]” may be imposed “under the laws of any State with respect to” data security, safeguards, investigations, mitigation, or notice. Such a provision will ensure that consumers will receive uniform protections, regardless of where they live, and will enable businesses to operate more efficiently, without the burden of having to comply with myriad state laws.
Outlook

Though the Senate Banking Committee is still to act on S. 3568, the House is now poised to bring an agreed-upon version of the three committee bills to the floor before the August recess. Even now, there are staff meetings taking place aimed at finding common ground that will allow for the issue to be debated and voted upon.

This Legislative & Public Policy Advisory is published by Alston & Bird to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. The material may also be considered advertising under the applicable court rules. Please contact any of the following attorneys for additional information or guidance:

Tom Boyd  
202-756-3372  
tom.boyd@alston.com

Paul Martino  
202-756-3439  
paul.martino@alston.com

Kathryn Marks  
202-756-3479  
kathryn.marks@alston.com

Dwight Smith  
202-756-3325  
dwight.smith@alston.com

If you would like to receive future Legislative & Public Policy Advisories electronically, please forward your contact information including e-mail address to legislative.advisory@alston.com. Be sure to put "subscribe" in the subject line.