Software & Information Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

COMMENTS OF THE

SOFTWARE & INFORMATION INDUSTRY ASSOCIATION (SIIA)

To the Notice of Proposed Rulemaking and Request for Public Comments on the

Health Breach Notification Rulemaking (Project No. R911002),

Pursuant to Section 13407(g)(1) of the American Recovery and Reinvestment Act of 2009

Submitted to the Federal Trade Commission (FTC) On June 1, 2009

On behalf of the members of the Software & Information Industry Association (SIIA), we appreciate this opportunity to comment on the Notice of Proposed Rulemaking and Request for Public Comments on the Health Breach Notification Rulemaking (Project No. R911002) ("Notice"), which was drafted pursuant to Section 13407(g)(1) of the American Recovery and Reinvestment Act of 2009 ("Recovery Act").

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet.[1] SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

SIIA has worked with regulators at the Federal and state levels in the United States, and also with policy makers in Europe, China, Canada and other regions, to examine the implications and operations of breach notification requirements since California enacted the first notification law in 2002. This has included work with the relevant federal

[1] Our website can be found at: www.siia.net

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

agencies implementing existing privacy and security regulations and policies (notably, the FTC's approach on unfair trade practices where companies fail to use appropriate technological means for protecting data, and as well as implementation of the Safeguard's Rule under the Gramm-Leach-Bliley Act), as well as state efforts (most notably, Massachusetts) to implement security measures.

Our comments on the above referenced Guidance takes into account these experiences and industry expertise.

PRELIMINARY OBSERVATIONS

SIIA was one of the first national organizations to call for a meaningful framework on breach notification, including efforts to promote on-going security practices and plans for firms. Over the course of the last several years, the need for a meaningful national framework has grown. On the one hand, the threats facing mainstream companies and institutions have gotten more complex and more sophisticated. Today, the threats are increasingly external to their operations, and driven by global crime and economic fraud perpetrators. Indeed, last year, according to one recent study, "91 percent of all compromised records in 2008 was attributed to organized criminal activity."[2]

At the same time, the fragmentation of laws and regulations continues to make an effective offense against these pernicious threats more difficult, to the frustration of consumers, business and enforcement authorities. At the start of 2009, 44 states, the District of Columbia and Puerto Rico have implemented laws that create a divergent and patchwork approach. To make matters even more challenging and pathworked, at least 9 states have enacted prescriptive security requirements (or amended their breach laws to achieve the equivalent goal) which makes an effective front against this deeply challenging. [3]

In this regard, SIIA would note PHR-related entities and vendors of personal health records would still be obligated to comply with all other federal and state statutory and regulatory obligations that may apply following a breach involving health information, such as state breach notification requirements. In the view of SIIA, it is very likely that the Interim Final Rule will lead to potential conflicts with both state breach notification requirements and with the at least 9 states which have enacted security requirements

---

[2] "2009 Data Breach Investigations Report, A study conducted by the Verizon Business RISK team", p. 13. Available at: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf.

[3] As of January 1, 2009, these states are: Arkansas, California, Maryland, Massachusetts, Nevada, Rhode Island, Oregon, Texas and Utah.

(or amended their breach laws to achieve the equivalent goal). The issue is not merely multiple compliance obligations, but potentially *conflicting* obligations which range from timing and content of notification, to the standard for determining a breach, to whether the information has been secured, etc. We believe it is inevitable that the FTC, working with HHS, will have to address this potential for conflicting compliance obligations in its proposed Interim Final Rule.

SIIA recognizes that the FTC has undertaken this Notice and Comment process based on statutory language that it was given by Congress. By any measure, this langauge is far from clear on many points, and is ripe with potential confusion. We note that this is the first federal statute to provide for breach notification; thus, there are very likely to be issues raised now and as this Interim Final rule is implemented that have not had to be addressed before by Federal agencies. In this regard, SIIA urges the FTC, in conjunction with HHS, to engage in some public consultations\round tables as the implementation date nears, given the complexity of this area and the possibility of ripe confusion for vendors, PHR-related entities, and other stakeholders.

SIIA offers our specific comments and looks forward to continuing to work with the FTC as the comments are considered, the Interim Final Ruler further is developed or if our experience in the industry can help address any questions that arise.

AVOID CONSUMERS RECEIVING MULTIPLE BREACH NOTICES

The FTC inquires whether there are circumstances in which "a dual role [where vendors of personal health records and PHR-related entities may be covered as a business associate of a HIPAA-covered entity as well as covered as a direct provider of personal health records to the public], might lead to consumers receiving multiple breach notices or receiving breach notices from an unexpected entity, and whether and how the rule should address such circumstances."[4]

SIIA seconds the potential for concern expressed by the FTC that there is a risk of a dual role that could lead to any possibility that consumers would receive multiple notices. Such a situation would be not only costly and redundant; it would not serve the underlying public policy goal of prompting individuals to take action to protect themselves. SIIA strongly believes that the FTC and HHS should make clear in their respective Interim Final Rules that where an entity provides breach notification as required under one rule, it need not provide additional notice for the same breach because of the risk that it is covered by duplicative requirements implementing the relevant section of the Recovery Act.

[4] Section II. Section-by-Section Analysis, Proposed Section 318.1, p. 7.

As noted above in our preliminary observations, the myriad of state laws have created a patchwork that makes it very likely that the potential concerns expressed by the FTC on this point will also be made manifest. If vendors of personal health records and PHR-related entities (as well as HIPAA-covered entities and their business associates) notify under the Interim Final Rules, then it is extremely likely that they will have to notify individuals in the 44 states where separate breach notifications exist, and that the requirements for the notification in those situations are neither cotemporaneous nor identical. As a specific step, the FTC should recognize the potential for this duplication and conflict, and work to the greatest degree possible to avoid individuals receiving multiple notices regarding the same breach incident.

CLARIFY THE DEFINITION OF BREACH OF SECURITY

As SIIA understands the draft Interim Final Rule put forward by the FTC, the FTC intends to implement the statutory language defining a breach of security by distinguishing between "access" to PHR identifiable information and its "acquisition." Thus, "unauthorized persons may have access to information if it is available to them … [while] the term acquisition, however, suggests that the information is not only available to unauthorized persons, but in fact has been obtained by them."[5]

As a preliminary starting point in defining when a breach has occurred, SIIA concurs with the reading of the statute by the FTC. Without distinguishing between mere access and acquisition, the Interim Final Rule would result in unnecessary and harmful over notification to consumers, which have proven to be a significant problem, as discussed further below.

SIIA also concurs with the FTC approach that "the entity that experienced the breach is in the best position to determine whether unauthorized acquisition has taken place," and that the entity can rely on evidence "showing that the information was not or could not reasonably have been acquired,"[6] though in some important instances (discussed below), a third party may not be in the position to make a final determination of what health related information has been possibly been breached without a judgment from its client-vendor or client-PHR-related entity.

SIIA offers several observations on this point. First, the examples used by the FTC in the Notice include indicia that may not be particularly relevant to an entity determining whether, in fact a breech had occurred. For example, in scenario (3), the FTC includes the term "inadvertently" and the phrase "realized it was not the one he or she intended

[5] P. 8.
[6] P. 9.

to view" as apparent conditions to its conclusion that "breach notification was not required." In our reading of the statute and the FTC elaboration of the definition of breach, the references are, at best, confusing, and would suggest that an entity determine the *state of mind* of an employee before making a judgment about whether a breach has occurred. This is not inherently required by the statute, and may diminish the objective test otherwise laid out by the FTC.

Moreover, the use of the phrase "reading" in the scenario is inconsistent with the statute which requires a determination that there has been acquisition. Mere "reading" of a record, in and of itself, should not trigger notification requirements under the Interim Final Rule as it is related to mere "access" and *not* the "acquisition" of the information. In this regard, SIIA notes that the California Office of Privacy Protection, which has produced guidance implementing the nation's first breach notification law, and which has deep experience in what "acquisition" means, laid out the following useful considerations which are relevant here:

> "In determining whether unencrypted [the operative term in the California statute] notice-triggering information has been acquired…consider the following factors, among others:
> 1. Indications that the information is in the physical *possession and control* of an unauthorized person….
> 2. Indications that the information has *been downloaded or copied*.
> 3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported."[7]

SIIA strongly urges the FTC, consistent with the above analysis and the focus on acquisition – the operative term in the Recovery Act – to utilize action steps (like using, disclosing, downloading, etc.) in its definition.

Second, for purposes of the definition of "breach", SIIA notes that the "acquisition" standard raises the distinct possibility that information that has been redacted, truncated or obfuscated could be an objective measure that information could not reasonably have been acquired. We note that the standard for determining whether an "acquisition" has occurred is distinct from the statutory language that requires notification of unsecured PHR identifiable health information of an individual. Thus, consistent with the examples provided by the FTC in its Notice and consistent with the notion of "acquisition", we urge the FTC to incorporate the concept that information that cannot viably be accessed (such as through the aforementioned techniques) cannot be acquired.

---

[7] California Office of Privacy Protection, "Recommended Practices on Notice of Security Breach Involving Personal Information", Rev. May 2008, p. 12, available at: http://www.oispp.ca.gov/consumer_privacy/pdf/secbreach.pdf.

Third, with regard to the "evidence" cited in the FTC commentary as to what could ot could not reasonably have been acquired,[8] it is not customary in the industry to log ever instance of logging in or sign-in sheets. Moreover, the FTC should also recognize that this points to the utility of access controls – which is a distinct issue from whether the information has been de-identified – in determining whether there has been unauthorized acquisition.

Fourth, the Interim Final Rule will promote overnotification unless it makes clear that there are certain categories of transfers of health information by a vendor or PHR-related entity that are necessary to the subsidiary or affiliate services that an individual expects from the vendor or entity and which do not constitute a each transfer of health information giving rise to unauthorized acquisition. These transfers are inherent to the authorization given by an individual in the context of the nexus with the vendor or entity. As such, it would be unreasonable for an individual to expect to give each such transfer individual authorization. It is appropriate, the, for the definition of breach not to include such subsidiary or affiliate transfers and the corresponding authorizations from the vendor or entity to facilitate such transfers. To state the obvious, if the consent of the individual is required each and every time such an otherwise authorized transfer occurs, this raises both impractical operational issues and potential notification triggers that would lead to over notification.

THE DRAFT INTERIM FINAL RULE SHOULD RECOGNIZE THE RISK OF SERIOUS OVERNOTIFICATION TO INDIVIDUALS

As the FTC is well aware, there is a serious policy consideration that a notification framework:

> "… might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, ***notices may be more common than would be useful***. As a result, ***consumers may become numb*** to them and fail to spot or act on those risks that truly are significant. In addition, ***notices can impose costs on consumers and on businesses,*** including businesses that were not responsible for the breach. [Examples given.] Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[9]

[8] Page 9.
[9] Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the United States Senate (June 16, 2005), p. 10. Found at: http://www.ftc.gov/os/2005/06/050616databreaches.pdf. (Hereinafter referred to as "Majoras Testimony."

Similar concerns were expressed in April 2007, by the Identity Theft Task Force, comprised of 17 federal agencies with the mission of developing a comprehensive national strategy to combat identity theft, and which reinforces a key consideration in the protection of consumers: *There may be direct and harmful unintended consequences that may be associated with broad notification*. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications. The concern is based on the fact that consumers are being preyed upon by bad actors following massive notifications. In January 2006, the New York State Consumer Protection Board (CPB) advised that scam artists were trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already be the victims of identity theft.[10] The FTC was compelled to caution U.S. veterans in 2006 "to be extra careful of scams following the recent data breach at the Department of Veterans' Affairs (VA)," noting that "[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the phone."[11]

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, referencing recent news reports of "breaches", asking them to enter their details and account numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user's account and against the backdrop of the most recent data breach, many users will assume that news is legitimate.[12]

As a general matter, even in this area of sensitive personal information and taking into account the specific statutory definitions found in the Recovery Act, SIIA urges the FTC to recognize that nothing in the Interim Final Rule is meant to undermine that consistent element of FTC statements and policy.

---

[10] See "Phishing Fraudsters Prey on Identity Theft Fears," January 13, 2006, found at: http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html.

[11] "FTC Warns Veterans to Delete Unsolicited E-mails;*Scams via E-mail and Telephone Often Follow Data Breaches*," (June 2, 2006), found at: http://www.ftc.gov/opa/2006/06/fyi0632.htm.

[12] See "Will MasterCard breach breed new wave of phishing?", 21 June 2005. Found at: http://software.silicon.com/security/0,39024655,39131331,00.htm.

THE FTC SHOULD NOT INCORPORATE THE 'GUIDANCE' ISSUED BY HHS WITHOUT FURTHER ADJUSTMENTS

SIIA notes that the FTC appears to incorporate wholesale into the draft Interim Final Rule the Guidance issued by HHS in April regarding the technologies or methodologies that it determined made information unusable, unreadable or indecipherable. We will not repeat all of the arguments here, but simply state our observation, detailed in our attached comments, that "there is much work to be done on this Guidance before it is finalized prior to the implementation of the interim final rule. The comments [submitted by SIIA] recommend concrete steps to reflect the diversity of the entire information management cycle that is now touched by this dramatically expanded coverage of health information under the Recovery Act, as well to achieve the goal of the legislation not to focus on too narrow a set of technologies and methodologies."

We note, in particular, our comments therein on other approaches, which FTC inquired about in its Notice.[13]

THE FTC'S TREATMENT OF THIRD PARTY SERVICE PROVIDERS IN PROVIDING NOTICE: SOLID APPROACH, WITH IMPORTANT CLARIFICATIONS

As SIIA understands the FTC proposal, in the event a third party service provider to a vendor of personal health records or PHR-related entities experiences a breach of security, the obligation is on the third party service provider to notify their respective clients, the vendor or PHR-related entity, and not the affected individuals directly.

SIIA concurs with the FTC's general approach, as it serves to facilitate the notice coming from the vendor or entity that the individual has the relationship with. Otherwise, consumers would be receiving notices from entities they may never have heard of, or pose requirements that fundamentally disrupt the relationship between the individual and the vendor or entity.

SIIA urges several concrete changes to the approach in the proposed Rule that are consistent with the statute and the approach of the FTC. First, proposed paragraph 318.3(b) requires that the third party service provider's notification shall include the "identification of each individual" whose information "has been, or is reasonably believed to have been acquired during such breach." From our industry's experience in managing information for clients, and our experience with prior breaches, third party processors often do know what kind of data they process for their clients. Thus, it may not be possible – indeed, it may be impossible – to identify "each individual." More often than not, the situation following a breach will involve the third party service

[13] P. 13.

provider consulting with the client-vendor\PHR-related entity to determine if, in fact, there is personally identifiable or who the affected individuals would be.

Second, the proposed Interim Final Rule micromanages who should be contacted. As an industry practice, a third party service provider will have already identified, through contract, the appropriate point of contact to work with in the event of a breach. That reflects the on-going nature of the relationship and the need to have 'on the ground' operations work effectively and efficiently. Whether that person is a "senior official" of the vendor or PHR related entity is irrelevant, and will depend on the nature and size of the organization. We would strongly urge that the proposed paragraph be adjusted to reflect that contracts should specify the approach points of contact and, if not otherwise provided, then a senior official.

Third, the FTC needs to clarify that the term 'maintains' in the definition if Vendor of personal health records is a narrow category and is distinct from the 'maintains' element of the definition of 3rd party service provider. The key is to ensure the fundamental character of which entity has the relationship with the individual whose health information is being collected, 'maintained', etc. Nothing in the FTC Interim Final Rule should adopt a definition of 'maintains' that brings Third party service providers into the nexus that is inherently that of the vendor.

Fourth, the "identification of each individual" raises another concern, one which SIIA assumes that the FTC did not intend. Where a breach affects a third party service provider, there is the possibility that multiple Vendors or PHR-related entities may be affected. As currently written, the relevant section of the Interim Final Rule would require a third party service provider to provide the identification of each affected individual to all such entities. This would, of course, exacerbate an already problematic situation. Thus, where multiple vendors or PHR-related entities may be affected, the Rule should clarify that the third party service provider, to the degree it is able (consistent with our analysis above) to provide the particular information should only do so to the Vendor\PHR-related entity which owns and licenses the particular breached information.

COMMENTS ON 'PHR IDENTIFIABLE HEALTH INFORMATION': CLARIFICATION REQUIRED

SIIA summarizes several points below, in addition to the comments we've provided elsewhere in our submission.

First, on page 11, there is reference to a "reasonable basis to believe" that information can be used to identify the individual. In our view, this point is directly connected to whether a breach has taken place, and is distinct from the formalistic approach of

recognizing only 'de-identification.' Indeed, if information has been redacted, truncated, obfuscated, *or otherwise pseudonymized (such as through assigning random identifiers to information)*, then there is no reasonable basis to believe that the information can be used to identify the individual. In this regard, SIIA urges the FTC to recall its longstanding concern with the harmful effects of overnotification mitigation the need for notice if there is a reasonable basis to believe that a Vendor or PHR-related entity cannot be used to identify the individual.

Second, on page 12, the FTC commentary uses the example of the Interim Final Rule covering a security breach of a database "containing names and credit card information, *even if no other information was included.*" (emphasis added) SIIA asks the FTC how, in this specific instance, this is HIPAA related and not related to other laws, such as Gramm-Leach-Bliley Act (GLBA)? In addition, this example reinforces the very real likelihood that there will be conflicting requirements imposed on vendors or PHR-related entities under the myriad of state laws.

Third, on page 18, the FTC provides further commentary on the "reasonably should have been known""standard, and reemphasizes the need for entities to maintain reasonable security measures. SIIA notes that the list includes only one example – breach detection measures. It is important that any list included in the FTC Rule or accompany commentary not proscribe a specific approach. In this specific instance, in the context of external 'incidental' access, such breach detection measures are virtually impossible, and there is virtually no way to find them using currently tools and techniques.

Third, on page 13, there is reference to specific identifiers being "removed." If this is a substitute for 'de-identification', then this is an unclear reference. Moreover, in the context of whether there is a 'reasonable basis to believe that information can be used to identity an individual,' SIIA notes the discussion, *supra*, of other techniques including pseudonymization.

COMMENTS ON THE DEFINITION OF PHR-RELATED ENTITY: CLARIFICATION NEEDED

In the first example, on page 14, there is reference to a brick-and-mortar company 'advertising' dietary supplements online. This example is confusing, as the FTC commentary does not explain how the act of 'advertising' corresponds with any element of 'PHR identifiable health information' or a 'personal health record.' In our view, mere advertising does not contain elements of either definition, and request that the FTC remove this example.

Second, in the third example, the FTC commentary states that this category includes "online applications." As commonly used in the industry, this term is quite broad and could potentially wrap in many common tools on the internet (such as a browser or other middleware software) that merely enables an application to work. SIIA assumes, in the context of this Interim Final Rule, that the FTC was not including any 'online application' that merely assists in the transfer or communication of heatlh information and is focused on whether the 'online application' has nexus to an individual and captures the relevant health information or record.

REMOVE 'EXPRESS AFFIRMATIVE CONSENT' TO THE REQUIREMENT FOR INDIVIDUAL NOTICE BY EMAIL

As the FTC states in its Notice, "email notice may be particularly well-suited to the relationship" between a vendor of personal health records or PHR-related entity; indeed, "vendors of personal health records and PHR related entities may not want to collect mailing addresses from consumers, and consumers may not want to provide them."[14] SIIA concurs with this analysis.

Despite these facts, the Notice specifies that an individual must provide "express affirmative consent" to receive notices by email. In our view this is inconsistent with the FTC's analysis of the benefits of using email, and an inappropriate interpretation of the statutory phrase, "specified as a preference by the individual." The FTC's formalistic approach to the pre-checked boxes or disclosure is especially unwarranted. The fundamental consideration in the relationship with the vendor or PHR-related entity will be basis for a consumer's consent and choices, and *not* the decision about a *speculative matter* that may never occur, namely notice in the event of a breach of security. Thus, having pre-checked boxes or disclosures in this *collateral*, non-transactional basis of the relationship, is not only perfectly appropriate and consistent with many online business-consumer relationships, but could risk utter confusion if the vendor or PHR-related entity does not collect physical address information and the individual does not 'affirmatively' check the box for email notices.

[14] P. 21.

THE 'NOTICE TO THE COMMISSION': FURTHER WORK IS NEEDED

The draft Interim Final Rule indicates that in the event of a breach, vendors of personal health records and PHR-related entities must notify the FTC as soon as possible (in no case later than 5 days) after discovery of the breach if the unsecured PHR identifiable health information of 500 or more persons is involved. If fewer than 500 persons are involved, the entities are to maintain a breach log which it must submit annually to the FTC.

SIIA notes that this will be the first effort by any agency of the Federal government to require specific notice in the event of a breach. As such, it can be anticipated that there will be many unanticipated problems and challenges that arise from this requirement.

With regard to the FTC's intention to develop a form to be posted on its website to be used by entities to provide both immediate and the annual notice, SIIA expresses some doubt that the form will prove appropriate for many circumstances. It is likely that a rote form posted publicly will facilitate robotic submissions, many of which may not be relevant. It is also likely that the database which will maintain these forms will be the subject of intense efforts by hackers.[15] SIIA would urge the FTC, as an alternative to designate a point person or office to receive notices (which may utilize a form), either by registered or express mail.

Regardless of the manner in which the information is received and transmitted, SIIA strongly urges the FTC to treat any and all such information as business confidential, not subject to release under FOIA, and with the potential to be evidence in a criminal or civil proceeding.

Taking into account our assessment of the experiences of our industry following a breach, a critical challenge the FTC will face is how to ensure effect coordination among agencies. As stated in our preliminary views, many breaches involve criminal or illicit activity, which brings into action a variety of agencies, at both the Federal and state levels. As the FTC implements its particular notice requirements, it should ensure that these processes are not interrupted, and indeed, encouraged and facilitated consistent with its statutory mandates.

[15] The potential for hackers to access sensitive data bases was examined by the FTC in "The National Do-Not-Email Registry: A Report to Congress," June 2004, available at: http://www.ftc.gov/reports/dneregistry/report.pdf. See discussion at p. 16.

NOTICE TO INDIVIUDAL BY 'TELEPHONE': ENSURE NO CONFLICT WITH THE DO-NOT-CALL LIST

In the proposed Interim Final Rule, the FTC would allow a vendor or PHR-related entity to provide notice by telephone, in addition to notice by email, if there is possible imminent misuse of unsecure PHR identifiable health information.[16] Such telephone notice may include services, products or other "steps" individuals should take to protect themselves from potential harm, as well as contact procedures for individuals, including reference to a toll-free telephone number, email address, website or postal address (which may include advertising or references to other service or products). The FTC should make very clear that any such telephone notice under this Rule does not constitute a violation of any "Do-Not-Call" list, either the national registry or internal company lists.

CONTENT OF NOTICE: AVOID UNINTENTIONAL HARMFUL CONSEQUENCES

In its commentary on the content of what should be included in the Notice, the FTC states that the notice should include "a description of how the breach occurred."[17] The proposed Rule differs slightly in its formulation, stating the notice should include "a brief description of how the breach occurred."[18]

SIIA notes that the language in both the commentary and the proposed Rule differs substantially from that of the statute, which more generally requires notice to include "a brief description of what happened",[19] including the date of the breach and date of discovery of the breach.

It is essential that the FTC follow the language of the statute more closely. Any notice that describes how the breach occurred would have serious unintentional consequences and give the bad actors (see discussion, *supra)* a roadmap to not only how to cover their tracks in the particular breach in question, but also for future breaches. Such a description may also jeopardize legal proceedings (as distinct from a law enforcement investigation). Moreover, the goal of informing individuals so that they can take action to protect themselves is served quite well by the language in the statute, and not by the detail proposed in the FTC Rule.

[16] Proposed 318.5(a)(2).
[17] Page 28.
[18] Proposed 318.6(a).
[19] Section 13402(f).

PAPERWORK REDUCTION ACT: GENERAL COMMENTS

In the second full paragraph, the phrasing fails to note the role, otherwise established in the Rule, of third parties notifying other entities. Thus, the sentence should read, "…and, if certain conditions are met, notify consumers, *other entities* and the Commission."

SIIA has reviewed the cost assumptions put forward by the FTC. For a variety of reasons, we believe the costs are underestimated by the FTC. First, it is very likely that the Rule will result in duplicative and potentially conflicting requirements. The costs of such duplicative efforts, and the time and resources to address conflicting requirements, is taken into account (or even acknowledged) in the FTC commentary.

Without comment on each and every assumption, SIIA will point out, by way of example, the FTC estimate that "on average, 100 hours of employee labor" may be at stake. It is our view, taking into account some of the real world experiences that have been shared with us following report of a breach, that 100 hours could be wracked up merely by internal corporate activities – which involve public relationship, security, marketing, legal, and remedial teams, as well as outside counsel, consulting (forensic and otherwise).

Finally, we note that the FTC's Interim Final Rule may, in fact, may be "temporary."[20] Depending on the results of the required study and submission of a report to Congress containing recommendations within one year of enactment of the Recovery Act, entities affected by the Interim Final Rule are likely to be subjected to uncertainty and potential confusion, as well as additional costs which are not included in the FTC's calculations.[21]

CONCLUSION

SIIA appreciates this opportunity to comment on this important rulemaking activity. Please do not hesitate to contact us if you any have any additional questions or need further information.

[20] See Section I. Background, p. 5.
[21] See Section IV. Paperwork Reduction Act, p. 30.