April 28, 2014

Via e-mail: rule-comments@sec.gov

Ms. Elizabeth M. Murphy
Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Re-Opening of Comment Period for Asset-Backed Securities Release
Release Nos. 33-9552; 34-71611; File No. S7-08-10

Dear Ms. Murphy:

The Structured Finance Industry Group ("SFIG")[1] appreciates the opportunity to comment on Release Nos. 33-9552, 34-71611 related to the proposed revisions to Regulation AB ("proposals").

On February 25, 2014, the Securities and Exchange Commission (the "Commission or "SEC") re-opened the comment period through March 28, 2014 for the proposed revisions to Regulation AB in Release No. 33-9117 (April 7, 2010) and Release No. 33-9244 (July 26, 2011), to permit comments on an approach for the dissemination of asset-level data as outlined in the staff memorandum concurrently released. On March 28, 2014, this comment period was extended to April 28, 2014.

This approach contemplates that the complete set of asset level data required under revised Regulation AB would be provided through an issuer or issuer-sponsored website and that asset level information that excludes potentially sensitive fields would also be filed on EDGAR. The Commission believes that under such approach, "issuers could determine for themselves the specific controls needed for the dissemination of sensitive information" on a website, in a manner that would result in "appropriate safeguards to comply with privacy laws."

SFIG thanks the Commission for the opportunity to comment on the proposed approach in accordance with the captioned release, and we are grateful for the extension of the comment period to April 28, 2014. The views expressed in this letter come from our membership, which includes issuers, investors, financial intermediaries, data and analytics companies, and other market participants. The SFIG membership believes that securitization is an essential source of core funding for the real economy. It connects investors with appropriate investments and provides consumers and companies with access to capital. Like any powerful tool, securitization must be used carefully, and thoughtful regulation is a part of that. We appreciate the effort by the Commission and staff to advance the proposed revisions to Regulation AB to finalization, and we look forward to working together in this regard.

[1] SFIG is a member-based, trade industry advocacy group focused on improving and strengthening the broader structured finance and securitization market. SFIG provides an inclusive network for securitization professionals to collaborate and, as industry leaders, drive necessary changes, be advocates for the securitization community, share best practices and innovative ideas, and educate industry members through conferences and other programs. Members of SFIG represent all sectors of the securitization market including issuers, investors, financial intermediaries, law firms, accounting firms, technology firms, rating agencies, servicers, and trustees. Further information can be found at www.sfindustry.org.

Executive Summary

The following is a brief overview of the key substantive comments and suggestions that we will make in this letter:

As mentioned above, we are grateful to the Commission for the opportunity to make comments on the proposed approach. However, because the proposed approach does not specify the exact asset level data fields to be required under revised Regulation AB, the proposal in effect lacks sufficient detail needed to elicit maximum industry engagement in the commenting process. As an organization that seeks to harmonize and build consensus among all industry constituencies, we believe that issuers, investors and other industry participants across all asset classes will not be able to derive fully thought out positions on the proposal absent that level of detail.

While we are submitting this letter in order to meet the April 28, 2014 comment deadline, we would very much appreciate the opportunity to provide further, more fulsome comments when we better understand which disclosures will be required. **Accordingly we request a partial re-proposal of the revisions to Regulation AB indicating what the final required data fields will be and requesting comment on a complete set of proposed rules regarding the issuer website proposal and related privacy issues, which will provide all commenters a further opportunity to comment on a more targeted and solutions focused basis**. Given the lack of clarity around the data fields to be required under revised Regulation AB, it is ultimately impossible to provide the industry's most fulsome commentary without a re-proposal.

With regards to the limited specifics of the proposal itself we would suggest the following:

In the case of many asset classes we believe that the proposal increases the likelihood that, taken in conjunction with other publicly available data, some previously anonymized data may be re-identified or de-anonymized, which possibility in turn gives rise to certain risks:

- Issuers may be subject to privacy law considerations and in fact could be deemed a credit reporting agency
- Users of the data, including investors, may be subject to a lesser degree of privacy law considerations regarding both the use and disposal of information
- All participants within the data "chain", by their very association with the data may, in the case of hacking or inappropriate use of data, be subject to reputational risk – such risk being associated not just with the industry participant, but also with any easily associated corporate parent, subsidiary or affiliate
- Borrowers may suffer harm if their data is re-identified and is used improperly

Considering the industry is commenting on a "blind" basis without any understanding of the specifics of the data fields being contemplated, then, without making any representations as to the appropriateness of those data fields, industry participants **believe it is essential that any disclosure requirements be coupled with interpretive relief protecting both issuers and investors from liability under various privacy laws, especially under FCRA**. Put simply – in order for markets to function at an optimal level, it is essential for providers of information (issuers) and receivers of information (investors) to be able to provide and receive information in a safe environment without fear of legal consequences.

Regarding reputational risk, we believe that the possibility of re-identification of anonymized data is highly fact specific and subject to change. We, therefore, do not have comfort that the risk of re-identification can be considered to be reasonably mitigated across all asset classes or that reputational risks can be fully remediated by the privacy law liability relief that we propose.

We would therefore request the Commission to consider alternative methods of delivery and alternative data retention periods as a potential basis for mitigating reputational risk.

We would also re-iterate the need for more clarity regarding the contemplated data fields. For certain asset classes where there is significant uncertainty around these fields, it is entirely possible that industry participants may be able to coalesce around the requirements of the proposal and provide industry consensus recommendations to the Commission that satisfy the Commission's disclosure needs while also taking steps towards mitigation of the above risks.

In relation to the access restrictions contemplated within the proposal, we would also highlight two key concerns:

- <u>One consequence of foreseeable access restrictions is that in practice in a public offering, some investors may not access the data, and **we request that this not lead to an "omissions" claim against the issuer**</u>.

- We also note that access restrictions are not intended to impose a duty of confidence on the accessing investor, and <u>**we request technical amendments to other rules to prevent such a duty arising**</u>.

In addition to the above key requests, we also note the following issues:

- Given the risks of legal liability for alleged violations of privacy law (as discussed in detail in our letter), if the issuer website proposal moves forward, we further indicate that issuers will need substantial latitude in setting access restrictions on their data websites. Conversely we also discuss investor concerns with the potential access restrictions, in terms of liability as well as ease of use.

- We also discuss cross-border implications of the proposed approach, in light of differences in privacy and consumer protection laws across jurisdictions.

- Finally, we discuss certain costs and burdens related to the issuer website proposal that we believe are not addressed in the staff memorandum.

1 <u>Need for a more detailed proposal</u>

At the outset, we note that it is difficult to comment on the proposed approach because there is a lack of clarity regarding the specific asset level data field requirements contemplated under the final revisions to Regulation AB. In the original proposed revisions, asset level data was proposed for several asset classes, including automobile, equipment and floorplan, and grouped account disclosure was proposed for credit cards. The Commission's response, as yet not known to the industry, to comment letters requesting changes in the granularity of disclosure for these asset types is essential to a considered analysis of the staff memorandum.

SFIG recognizes that many of its members, either individually or as part of various industry groups, have submitted comments in the past regarding the appropriate levels of disclosure, particularly in the area of loan level data. Recognizing the limited timeframe that the industry has been given to comment regarding the staff memorandum, our members have sought to restrict their comments solely to the issues relating to the newly proposed "issuer website". Notwithstanding this specific focus, the comments set forth in this letter by no means represent any withdrawal of positions previously expressed either in favor of or against certain levels of data disclosure, although it should of course be recognized that any such previously expressed positions may very well have been altered due to many factors including the passage of time.

Furthermore, there are important uncertainties as to specific data fields that will be required, for example with respect to residential mortgage loans. On the one hand, we could comment on the proposed approach assuming that the final rules will follow the April 2010 proposal and require disclosure of coded ranges (not specific values) for sensitive fields such as credit scores, monthly income and debt levels, and will also will not require zip code. However, the staff memorandum indicates that under the proposed approach some of these fields may be made more precise, and specifically suggests that the final rules may require disclosure of specific credit scores, monthly income and debt levels instead of coded ranges. Also it is uncertain what level of geographic granularity will be required under the final rule, as this factor is not addressed in the staff memorandum. This factor alone could have a significant impact on the ability to potentially re-identify borrowers from asset level data, thereby highlighting the privacy concerns with such disclosures.

A further uncertainty is whether the final revisions to Regulation AB will include the requirements, as proposed, that in offerings of structured finance products in reliance on Rule 144A (or Rule 506 or Regulation D) issuers provide to investors on request the same information that would be required in a registered offering. If this requirement is included, then issuers and underwriters will have to grapple with these issues in those offerings as well. We note that the staff memorandum mentioned issuers and investors moving to private deals to avoid costs of providing and receiving asset level information on websites, but we are not sure how to interpret or respond to those remarks in light of the original proposal regarding Rule 144A offerings.

Accordingly, there is a substantial lack of specificity around a key element of the approach outlined in the staff memorandum, that is, the specific asset level data fields that will be required by the final revisions to Regulation AB to be posted on the issuer website. This greatly limits our membership's ability to provide the Commission with more specific and constructive comments. The approach on which the Commission seeks comment lies at the intersection of federal securities law on the one hand, and consumer protection and privacy law on the other. These are two very different regulatory regimes, with fundamentally different purposes and objectives.

We appreciate that the intent of the proposed approach along with the proposed revisions to Regulation AB is that the asset level data fields to be required would not, on their face, identify the borrower. However, this comment letter addresses concerns that would arise if the asset level data fields, when combined by a user with other relevant and available data sources, could collectively contain information from which the borrower's identity could be derived (we refer to this process as "re-identification"). It is possible that there is a solution that will reconcile i) the objective of providing material asset level data disclosure to investors in accordance with federal securities laws, and ii) the need to protect borrower confidential information in compliance with consumer protection and privacy law, in a way that provides clear answers to issuers and investors on how to manage liability risks. However, we believe any such solution would be predicated on a specific set of facts and circumstances, including a precise set of asset level data fields.

We submit that any risk of borrower privacy violations that is not comprehensively resolved through regulatory action could create significant potential for litigation risk for issuers, and to some extent investors as well. A major reason for the lack of certainty in our comments relating to this matter is the lack of specificity on the asset level data fields that will be required under the final revisions. Many of our members have observed to the effect that without any insight into the specific asset level data fields that will be required, the prospect of commenting on the approach outlined in the staff memorandum is like commenting on a "black box" or an "invisible set of assumptions".

We would also respectfully observe that the staff memorandum is not a sufficient basis from which to draw comment and then proceed directly to a final rulemaking. The staff memorandum is more in the nature of a concept release than a proposed rulemaking. In particular, the staff memorandum does not include items such as the proposed rule text including conforming changes and technical amendments, the detailed discussion that normally would accompany proposed rule text, complete economic analysis including cost/benefit analysis, and so forth.

SFIG therefore believes that the Commission should request comments on the issuer website approach and related privacy considerations in the context of a formal rulemaking process, with adequate time for comment, that includes a complete description of the final asset level data requirements together with a final indication as to the requirement to provide in a Rule 144A offering the same information as required in a registered offering. Accordingly, we request a partial re-proposal of the revisions to Regulation AB indicating what the final required data fields will be and requesting comment on the issuer website proposal and related privacy issues, including a complete set of the final asset level data requirements as well as a full description of the issuer website proposal and related rule revisions.

2 Privacy law considerations

There are several state and federal privacy laws that would regulate or restrict the disclosure of the type of financial information that the SEC proposed revisions would require to be disclosed.

a. De-identification and Re-identification

Where information is not identifiable to any specific consumer, these laws generally do not apply. For example, under the Fair Credit Reporting Act (FCRA), the staff of the FTC has stated that information that is not consumer-specific is not a consumer report, even if the information is delivered in the context of a permissible purpose under the FCRA .[2] In an analogous context, the SEC, FTC and banking agencies, in promulgating the rule that requires secure disposal of consumer report information, stated that information that does not identify a specific consumer would not be subject to the rule's requirements.[3] Similarly, the federal Gramm-Leach-Bliley Act ("GLBA") rules, which prohibit financial institutions from disclosing consumer financial data to third parties, take an identical approach: information that is aggregated or "blind" and therefore is not personally identifiable is not covered by the rules and not protected from disclosure.[4]

The FCRA and GLBA, however, do not provide any guidance on when data should be considered to be "anonymized." The simplest method of anonymizing data would be to remove personal identifiers, such

[2] FTC Staff Opinion Letter from Clarke Brinckerhoff (June 3, 1987), *reprinted in* Ralph C. Clontz, Jr., Fair Credit Reporting Manual E-388 (1989 Supp.); FTC Staff Opinion Letter from Sheldon Feldman (August 27, 1973), *reprinted in* Ralph C. Clontz, Jr., Fair Credit Reporting Manual E-117 (rev. ed. 1977).

[3] See, e.g., 69 Fed. Reg. 21,388, 21,389 n.5 (Apr. 20, 2004) (preamble to proposed FTC Disposal Rule stating that "[i]nformation that does not identify particular consumers … would no longer be 'about a consumer.'").

[6] *See* 17 C.F.R. § 248.3(u)(2)(ii)(B).

[4] *See* 17 C.F.R. § 248.3(u)(2)(ii)(B).

as Social Security numbers, account numbers, mailing and property addresses, and names, and any other items that are "credit header record ".[5] Even when these identifiers have been removed, however, it still may be possible to associate data with a specific individual.

For example, an individual with statistically rare characteristics might be identified from even very carefully anonymized data.[6] One of our members has provided an example of this phenomenon: in Central and Lower Bucks County in Pennsylvania, there are 13 zip codes out of 53 in the area that had fewer than 20 homes sold in 2013, which would make it fairly easy to identify the borrower. In addition, our members report that it is extremely easy to identify an individual, especially the one that purchased one of the higher priced homes in the town in that calendar year. Another member indicated that for residential mortgages, given the zip code, loan amount and date of the mortgage, the borrower could be identified in the vast majority of instances just by reference to public records information (which is aggregated and made available by data vendors).

Another example: in the case of equipment loans, lenders perfect a security interest in collateral by filing a UCC financing statement, containing the name and address of the customer along with a description of the collateral. Filing dates for UCC financing statements are generally close to the origination date of the contract with the customer. State level UCC databases are generally searchable by creditor and anyone can order a UCC search for a fee. A person in possession of an issuer’s UCC filings, could merge that information with the types of loan level data identified in the Regulation AB proposal, including origination date, zip code and amount, to specifically identify by name and address the customer that is the subject of the issuer’s loan level disclosure. This specific identification could thereafter be used for improper purposes. In addition to presenting regulatory, compliance, and litigation risks, this also is of concern for reputational and competitive reasons.

Additional examples of re-identification may be provided for other asset types, such as auto loans and leases. However, without knowing the specifics of the data field disclosure contemplated by the Commission such examples would be hypothetical and the industry would be far better served focusing on a clearly defined and transparent proposal.

The SEC itself has been reluctant to provide a strict definition of when data has been de-identified. In its final rule regarding the disposal of consumer report information, the Commission stated, “We have not included a rigid definition [of information that would be considered identifiable] in the disposal rule … because, depending on the circumstances, items of information that are not inherently identifying can, in combination, identify particular individuals."[7]

Other privacy rules have addressed the issue of aggregation by proposing a flexible standard based on generally accepted statistical methodology. For example, the Privacy of Individually Identifiable Health Information Rule, promulgated under the Health Information Portability and Accountability Act (“HIPAA”), states that for information to be considered “de-identified,” a covered entity must have “no reasonable basis to believe that the information can be used to identify an individual” and a person with appropriate knowledge and experience of the technical principles of de-identifying information must determine that

---

[5] *See* id. (excluding from the GLBA definition of nonpublic personal information, data “that does not contain personal identifiers such as account numbers, names, or addresses”). Credit header record is the identifying information that accompanies consumers' credit reports. It consists of name, name variations, address, former addresses, telephone number (even unlisted numbers if known), date of birth (usually limited to month and/or year of birth) and Social Security number.

[6] *See, e.g.*, Federal Committee on Statistical Methodology, Office of Management and Budget, Statistical Policy Working Paper 22—Report on Statistical Disclosure Limitation Methodology at 20 (May 1994) (discussing the re-identification problems inherent in statistically unique variables).

[7] 69 Fed. Reg. 71322, 71324 (December 8, 2004).

there is a very small risk that the information could be used by others to identify a subject of the information.[8] Thus HIPAA requires a case-by-case determination, by an expert familiar with de-identification, that aggregated data cannot be reverse-engineered and “re-identified” with a particular consumer.

Similarly, the federal Census Bureau has implemented a case-by-case analysis for data aggregation. The Census Bureau is prohibited from publishing information that would allow any individual to be identified,[9] and, in response to this prohibition, has created a Disclosure Review Board, which examines every proposed Census publication, taking into account the sensitivity of the information contained, the statistical and other methods that have been applied to prevent identity disclosure, and geographical and other identifiers that have been retained.

The possibility of re-identification is highly fact specific, and depends on the asset type, the specific data fields that are disclosed pursuant to SEC regulations, the nature of relevant information that may be available in public records (which vary by jurisdiction and may change over time), the nature of information that may be available from data vendors and other providers (which also may change over time), and the nature of data that may be obtainable by improper or illegal means. After due consideration, if the rules were adopted as currently proposed SFIG believes that it will not be possible to reasonably mitigate the risk of re-identification. Given the vast amount of information that would be required to be disclosed under the SEC's proposal, the length of time over which the data must be made publicly available, and the dramatic advances in predictive modeling and data processing, we do not believe that the HIPAA standard or Census Bureau standard for de-identification would clearly be satisfied. That is, given the scope and nature of the data disclosure that would be required by the proposed Regulation AB II, we do not believe that a person with appropriate knowledge and experience of the technical principles of de-identifying information would be able to determine that there is a very small risk that the information could be used by others to identify a subject of the information.

The members of SFIG appreciate the SEC's efforts to protect consumer privacy through the removal of personal identifiers from the loan level data that would be required to be disclosed, but given the complexity of de-identification and re-identification explained above, we are unable to conclude that the data fields that would be required to be disclosed by the SEC's proposal would in fact be sufficiently de-identified in every instance. As a result, our comments presume that the data would be able to be identified to a specific individual, under at least some circumstances, and that there is a risk that the various state and federal laws governing the privacy and security of consumer financial data might be deemed to apply here.

b. Fair Credit Reporting Act

The most significant consumer privacy issues arise under the Fair Credit Reporting Act. We are concerned that the proposed approach outlined in the staff memorandum, might create a risk that the issuer, in posting the data fields on a website, could be considered a consumer reporting agency. As an example, to the extent that (among other criteria) the data posted are considered to be personally identifiable and contain data fields that were originally collected to assess creditworthiness in connection with an extension of credit for personal, family or household purposes, the data could be deemed to be a "consumer report". The consequences of such a characterization are that the very detailed and technical requirements of the FCRA may be imposed on the various participants in the securitization transaction, and that these participants may be subject to the especially draconian private right of action provided by the FCRA to consumers.

[8] 45 C.F.R. § 164.514(a).
[9] 13 U.S.C. § 9(a)(2),

If an issuer were considered a consumer reporting agency, it would be subject to numerous regulatory requirements and restrictions. For example, the issuer could disclose the data only to persons intending to use the data for a "permissible purpose," as prescribed by the statute, and the issuer also could be subject to specific rules relating to accuracy of data, disclosures of information to consumers, dispute resolution, and assistance to identity theft victims.[10] Moreover, because the data would consist of both public record and credit history information, and would likely relate to consumers residing nationwide, the issuer could be deemed to be a nationwide consumer reporting agency. As such, the issuer would be subject to a much more extensive set of restrictions and requirements, including the free disclosure of credit report information to consumers via www.annualcreditreport.com, which as a practical matter can only be satisfied by the three entities that actually are in that business – Equifax, Experian, and TransUnion.[11]

For users of consumer report information, such as the investors who obtain the information from issuers, the legal requirements include obtaining and using data only for a permissible purpose, notifying consumers when the user takes "adverse action" with respect to the consumer based on a consumer report, safeguarding data, and appropriate disposal of data received in order to prevent its misuse.[12]

The companies that provide information to consumer reporting agencies – known as "data furnishers" – also have specific duties to ensure the accuracy of the information that they report, and to investigate disputes with respect to the information that they provide to consumer reporting agencies.[13] In this context, "data furnishers" might include loan originators and servicers who provide loan and borrower data to issuers.

The challenges imposed by FCRA compliance are compounded by the major statutory damages, which are not capped, and a private right of action under the FCRA for non-compliance with its requirements. For negligent violations, a plaintiff can claim actual damages, as well as attorney's fees. For willful violations (including ones that involve a reckless disregard of the statute's requirements), there are statutory damages of up to $1,000 per loan, with no need to prove actual damages, in addition to attorney's fees and punitive damages. These kinds of claims have in the past been brought as class actions. In addition, there is no limitation on statutory damages under the FCRA, unlike other consumer credit laws, such as the Equal Credit Opportunity Act, the Fair Debt Collections Practices Act, the Electronic Funds Transfer Act and the Truth in Lending Act.[14] The combination of very technical statutory requirements, the availability of statutory damages and class actions, the absence of a limitation on class-action damages, and a high volume of transactions (in this context, issuers might be disclosing thousands or hundreds of thousands of consumer reports per securitization to investors) adds up to dramatic litigation exposure, even for claims that have little or no merit. In fact, courts have characterized the FCRA liability scheme as "ruinous," "annihilating," "crippling," and "catastrophic."[15]

[10] FCRA §§ 604, 605, 605A, 605B, 607, 609, and 611.
[11] FCRA §§ 603 (p)(defining "nationwide consumer reporting agency"); 612 (regarding annual free disclosures of credit reports).
[12] FCRA §§ 604, 615, 628.
[13] FCRA § 623.
[14] *See, e.g.,* Truth in Lending Act § 130(a)(2)(B) (capping class action damages); Equal Credit Opportunity Act § 706(b) (capping punitive damages in class actions); Fair Debt Collection Practices Act § 813 (capping statutory damages in class actions); Electronic Funds Transfer Act § 915(a)(2) (capping statutory damages in class actions).
[15] See, e.g., See Stillmock v. Weis Mkts., Inc., 385 F. App'x 267, 281 (4th Cir. 2010) (Wilkinson, J., concurring) (discussing the "annihilating liability" that can be imposed upon companies in the context of an FCRA class-action). Phillips v. Accredited Home Lenders Holding Co., 2007 U.S. Dist. LEXIS 59880 (C.D. Cal., May 15, 2007) (certifying class despite prospect of "crippling" damages).

Although a potential investor would have a "permissible purpose" to obtain consumer report information, in connection with valuing or assessing the risk of an existing loan,[16] the entity disclosing the information might still be considered to be a "consumer reporting agency," and the users and furnishers of such information might still be subject to the FCRA.

Although we believe strongly that securities issuers would not be considered to be consumer reporting agencies when disclosing loan level data to potential investors, given the high cost and risk of this type of litigation, there is a need for specific authoritative guidance in the context of the disclosures currently under consideration here. A "consumer reporting agency" is defined under the FCRA as a person who assembles data on consumers for the purposes of providing consumer reports to third parties.[17]To the extent that issuers may assemble data about consumers, they would not be doing so for the purposes of providing consumer reports to investors, but rather would be assembling data about consumers for the purposes of offering securities or complying with the SEC's Regulation AB II. The staff of the Federal Trade Commission has issued guidance supporting this position,[18] but, because this guidance is issued by the staff, not the actual Commission, and, because the FTC does not have formal rulemaking or interpretative power under the FCRA, this staff guidance is not fully authoritative.[19] Moreover, the shift in FCRA's primary regulator from the FTC to the Consumer Financial Protection Bureau (CFPB) as discussed below creates additional uncertainty.

Since the passage of the Dodd Frank Act there is now a single federal agency with the authority to make rules and to interpret the FCRA: namely, the CFPB. To date, the CFPB has neither ratified nor repudiated the interpretations of the FTC staff. Before the SEC follows through with the proposal to require issuers of securities to disclose this information to third parties, it should seek from the CFPB a rule or an authoritative interpretation of the FCRA that would permit securities issuers to disclose such data without subjecting themselves to any risk – regardless of how remote – of being deemed to have assumed the responsibilities and liability of consumer reporting agencies or, even more dramatically, to the duties of nationwide consumer reporting agencies.

The securitization industry simply cannot afford any legal uncertainty as to whether the data posted would be deemed a consumer report, or whether an issuer, as a consequence of complying with the revised Regulation AB disclosure rules, would be deemed a consumer reporting agency. At the most extreme level, there could be the potential for a penalty of $1,000 per loan if the issuer, if deemed a consumer reporting agency, fails to maintain procedures to ensure the "maximum possible accuracy" of the information being disclosed to investors, fails to provide a proper file disclosure to a consumer, or fails to provide statutorily required assistance to identity theft victims. This penalty, multiplied by the potentially

[16] FCRA § 604(a)(3)(E). We note, however, that certain states also have adopted credit reporting laws, including requirements that credit report information be disclosed only for a permissible purpose, and those states may not include potential investors among the permitted recipients of consumer report information. See, e.g., California Civil Code § 1785.11 (California credit reporting law does not expressly address disclosures to potential investors among the permissible purposes).

[17] FCRA § 603(f).

[18] *See* "40 Years of Experience with the Fair Credit Reporting Act, and FTC Staff Report with Summary of Interpretations," at 30, Comment 603(f)-4.D (stating that an entity that transmits consumer information to an actual or potential successor in interest, including a participant in a securitization, does not become a "consumer reporting agency," because its purpose is not to provide consumer reports, but rather to consummate the securitization transaction); *id*. at Comment 603(f)-4.C (stating that a creditor does not become a consumer reporting agency by providing consumer information in order to comply with rules and other applicable legal requirements); *id*. at Comment 603(f)-4.B (a creditor does not become a consumer reporting agency by communicating consumer report information about an applicant or borrower to an entity that "must participate in the transaction in order for it to be completed").

[19] *Hartman v. Lisle Park District*, 158 F.Supp.2d 869, 876 (N.D.Ill. 2001) (holding that FTC staff opinion letters interpreting the FCRA are entitled to respect "only to the extent that those interpretations have the power to persuade").

tens or hundreds of thousands of loans per securitization transaction for some asset types (auto loan ABS include as many as 75,000 loans per deal) and the ongoing monthly reporting on the tens of thousands of loans, would be significant. To put a finer point on this example, an auto issuer could be faced with a potential liability of $75M for a single auto loan securitization. Student loan ABS may include up to 400,000 loans per securitization. While the likelihood of this liability is remote, the magnitude is very large, and could lead to a reduction in securitization issuance which could result in a possible contraction in consumer credit.

In view of the risks posed by even the possibility of a finding of FCRA violations, we believe that the proposed approach described in the staff memorandum would not be workable, unless the CFPB first implements a regulatory change or issues an authoritative interpretation under FCRA making it clear that the data posted by the issuer in compliance with the revisions to Regulation AB or other legal requirements would not be considered a consumer report, and that the issuer or any person providing any such data would not be considered to be a consumer reporting agency.

c. Other Data Privacy and Security Rules

In addition to the FCRA, the SEC's proposal implicates other data privacy and security requirements. We believe that these provisions generally may be accommodated, because they include specific exceptions to address these types of disclosures, and are not subject to statutory damages schemes.

For example, the SEC's privacy rule under the Graham-Leach-Bliley Act ("GLBA") prohibits the disclosure of personal financial information to third parties, but permits such disclosure "in connection with a proposed or actual securitization, secondary market sale, or similar transaction relating to a transaction of the subject consumer."[20] We would nonetheless request that the SEC clarify in any final rulemaking that the disclosure of information by issuers to investors in compliance with the revisions to Regulation AB is permitted by this, or other, exceptions under GLBA.[21] Because issuers may be subject to multiple agency privacy rules under GLBA, including rules of the banking agencies or the CFPB, we further request that such clarification with respect to the applicability of these exceptions under the GLBA privacy rule to the disclosures required by the revisions to Regulation AB be provided through coordinated interagency action by the SEC, the CFPB and all other agencies that administer GLBA privacy rules.

Issuers also may be subject to disclosure restrictions under state laws, such as the California Financial Information Privacy Act.[22] Again, however, certain of these laws specifically permit disclosures in connection with securitizations.[23]

Federal and state data security requirements, under GLBA and other laws, are similarly implicated by the SEC's proposal. These requirements typically require financial institutions, such as issuers, to evaluate the risks to consumer data within their organizations, to develop and implement written plans to address those risks, and to regularly evaluate those plans to ensure that they are continuing to meet their intended purposes.[24] In this case, the SEC's proposal would result in significant risks to consumer financial data, because of the disclosure of a great deal of detailed data to a multiplicity of investors. This data will need to be transmitted, displayed, and accessed in a secure manner, to investors who are known to have a

[20] 17 CFR § 248.14(a)(3).
[21] Other exceptions that might be applicable to the disclosure of loan level information by issuers to investors include disclosures to facilitate transaction that the subject consumer has requested; disclosures that are usual appropriate or acceptable to record, service, or administer the subject consumers account; disclosures that are required to comply with applicable legal requirements; or disclosures for required institutional risk control. 17 CFR §§ 248.14 and 248.15.
[22] Cal. Fin. Code §§ 4050 et seq.
[23] Id. at § 4056(b)(1).
[24] 17 CFR § 248.30.

legitimate investment need for the information and who are able to maintain adequate security for the data.

The proposed issuer website approach comes in the midst of increasing regulatory scrutiny on cybersecurity risks. For example, on April 15, 2014, the SEC's Office of Compliance Inspections and Examinations issued a Risk Alert describing its examination program to assess cybersecurity preparedness in the securities industry. This development simply underscores the fact that any issuer or issuer-sponsored website utilized under the proposed approach would be subject to intense regulatory scrutiny. The FDIC is also very focused on the cybersecurity issue, and recently has published statements urging financial institutions to be vigilant to risks and to utilize available government resources to detect cybersecurity risks.[25] And, in a recent speech on the topic, Comptroller of the Currency Thomas Curry stated: "Finally—and perhaps most importantly—we are concerned about the access third parties have to large amounts of sensitive bank or customer data. For an industry in which reputation means everything, a single data breach involving confidential customer information can be extremely costly. Banks are particularly vulnerable to events that erode trust, and once an institution's reputation is damaged, it can take years to repair."[26]

d. Reputational Concerns

All of the above also carry reputational risks for issuers and investors alike. Separate and apart from legal risks, we cannot emphasize enough that reputational risks associated with the proposed approach are very daunting, and loom large in our considerations both for issuers and investors alike. We are troubled by the risk that (in addition to potential class action or other liability) a well-intentioned issuer or investor could be subjected to criticism, have its image tarnished, be subjected to inquiries or investigations, or lose business opportunities simply because it was in the chain of custody of asset level data, that was subsequently misused by another party including by re-identification, hacking, accidental or intentional unrestricted release, or otherwise. Recent events indicate that the American public has little patience for having their personal information compromised through data breaches, and the reputational harm can indeed be severe. It should be recognized that reputational risk is by no means restricted to the specific legal entities that participate in a securitization transaction and extends through the full parental, subsidiary and affiliate organizational structure of any impacted party. Investor risk may extend through pension funds and insurance companies, issuer risk can extend from an auto finance company through to the manufacturer impacting the production of vehicles and the employment of US workers, or from bank issuers through the full bank corporate structure impacting consumer deposits and loan products. In short, there are multiple key aspects of the national economy that can be negatively impacted as a consequence of reputation risk created by the proposed housing of data contemplated in the staff memorandum.

While this comment letter will, in the following sections, focus on the need for privacy law protection and access restrictions we would highlight that, even if legal liability risks resulting from the proposed approach are viewed as minimal or can be substantially mitigated through features such as the FCRA rulemaking or interpretation, the reputational risk pertaining to potential re-identification of private data is virtually impossible to fully eliminate.

Specifically in the case of the market for RMBS backed by mortgage loans on U.S. properties, the industry is generally in agreement as to what a market standard for disclosure should be. Reputational

---

[25] FDIC Press Release, "FDIC Urges Financial Institutions to Utilize Available Cyber Resources", April 10, 2014, located at http://www.fdic.gov/news/news/press/2014/pr14028.html
[26] Remarks by Thomas J. Curry, Comptroller of the Currency, April 16, 2014, located at http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-59.pdf

risk must therefore be managed by mitigation efforts that actually reduce the risk of privacy breaches and enhance the chances of data remaining protected. In this regard, we would draw the Commission's attention to an FTC report from March 2012 that highlighted best practices related to data privacy. One principle recommended in this report is that "companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy."[27] Comments regarding data protection were provided to the FTC by different groups including businesses, trade associations, and consumers. The FTC ultimately recommended that companies "implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected."[28] We would point out the stark contrast between these data retention requirements and the need to retain data for a full 5 years under the Commission's proposal. In fact, not only is the retention period in contrast with the recommendations of the FTC, but the very idea of posting data publicly to a website versus the alternative of distributing information to qualified buyers presents a reputational risk that could be significantly reduced were the distribution alternative adopted.

With regard to other asset classes there may not be generally established practices as to the provision of specific loan level data. In addition to the above points regarding public website posting and length of time that information is displayed, we would also therefore emphasize that once the industry understands the specifics of those contemplated data fields, there may be further opportunity, without revisiting the arguments around the need for loan level data, for industry constituencies to coalesce around such data fields and determine opportunities to minimize the risks of privacy breaches. Upon clarification of those required data fields by the Commission, we would request that the relevant industry participants be given the opportunity to digest such requirements and make appropriate recommendations to the Commission as to how that risk can be best mitigated. Certain issuers could also be subject to risks related to the release of sensitive data that could be misused by competitors. For example, certain equipment and auto ABS issuers are captive finance subsidiaries of manufacturers. As such, they have direct competitors whose treasury departments' investment desks, as investors in those ABS, could gain access to information such as equipment prices and loan terms. A manufacturer, its dealers and its captive finance subsidiary could all be harmed as a result of its competitors gaining access to such information. These concerns are present even if access restrictions are imposed on the issuer website for asset level data, as discussed in section 4 below.

3 <u>Need for privacy law protection; changes from practices to date under the proposal</u>

Past and current practices in the provision of loan level data to investors in asset-backed securities are not indicative of the potential for privacy law liability in the future, under the revised approach and under Regulation AB as proposed, due to changes in dissemination practices that will inevitably result if loan level data is required across the board in registered offerings.

Actual practices to date in providing asset level data for asset-backed securities have varied significantly by asset class.

For residential mortgage loans and private label RMBS, investors have relied upon and issuers have provided asset level data (with name, address and other directly identifying fields removed) at or after the time of issuance directly or indirectly through various means. These means include direct provision of a

---

[27] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, at 23-30 (March 2012), located at http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[28] Id. at 28.

data file, uploading the data file to various third party analytics services, inclusion of a loan schedule in the transaction documentation, and posting asset level data on a trustee or master servicer website. Generally, if the issuer has determined that such asset level data is not anonymized and contains fields requiring protection for consumer privacy reasons, direct access to such data is limited to investors or prospective investors. Also, where websites have been used to provide data, if the issuer has determined that such asset level data is not anonymous and contains fields requiring protection for consumer privacy reasons, the websites have been password protected with access provided only after a user agreement has been signed. In these situations, the data is provided to a limited number of known, institutional investors, the user agreement creates confidence that the data will not be used for purposes other than evaluating the investment, and the data is not made available in a way designed to provide broad unrestricted access. Alternatively, where such asset level data is not viewed as containing fields requiring protection for consumer privacy reasons, access to the data may be unrestricted. We further note that, since 2008, most new offerings of private label RMBS have been made under Rule 144A, in which case investors that can access loan level data directly are limited to qualified institutional investors[29].

For other asset classes, such as credit card, auto loans, equipment loans, student loans, and dealer and equipment floor plan, there is not as specific a history in providing asset level data. Public auto loan transactions, for example, have not traditionally included asset level disclosures. It is only recently for certain Rule 144A offerings of subordinated classes that limited asset level data has been made available. It is our understanding that in asset-backed securitizations to date, for all asset types other than mortgage loans, asset level data has not been provided to investors in classes that were publicly offered, and has only been provided in classes offered under Rule 144A or in other non-registered offerings. Without opining on the appropriateness of asset-level disclosure for these asset classes, however, both the form of disclosure and the way in which it is shared, must take into account privacy considerations.

While some of these practices (particularly as to residential mortgages) have existed for some time, there are reasons why there is more sensitivity today to the risk of liability resulting from misuse of the data to re-identify individual borrowers.

First, as discussed above, most new offerings of private label RMBS are made under Rule 144A, and for asset types other than mortgage loans asset level data is provided only in classes offered under Rule 144A or in other non-registered offerings. Qualified institutional buyers in Rule 144A offerings are of a level of sophistication and have sufficient resources that they can be reasonably expected to have appropriate data safeguard procedures in place as required by federal and state data security and privacy laws. Moreover, in practice for a Rule 144A offering, asset level data access is limited to those specific qualified institutional investors participating in the initial offering, or that purchase in secondary trading which is generally conducted by a broker dealer that was involved in the initial offering. The involvement of the broker dealer interfacing with investors has the effect of limiting the persons accessing the data to actual investors (or, where applicable, prospective investors) in the specific security that are known to the broker dealer. As a result, in many cases only a few dozen investors actually have access to the data for any given securitization. But the proposal outlined in the staff memorandum would potentially give access to the asset level data to any investor or prospective investor, which in a public offering could mean any individual, meaning millions of persons could potentially request access to the data. Even assuming access restrictions of the type outlined in section 4 below, in a public offering the number of

[29] Prior to 2008, in registered offerings of RMBS, it was common practice to file anonymized loan level data on EDGAR. However, given the greatly reduced volume of registered RMBS offerings in recent years, such filings are very rare today.

prospective investors who could go directly to the issuer website (with no intermediation by a broker dealer involved in the offering or conducting secondary trading) and qualify for access could be in the tens of thousands or more depending on the access restrictions. Access restrictions on an issuer (or other transaction participant) asset level data website that are viewed as sufficient in a Rule 144A offered or restricted security[30], where there is a broker dealer involved in conducting the offering or secondary trading that acts as a gatekeeper limiting the investors that can obtain access the website, would likely not be sufficient in a public offering where any person could go directly to the website and self-certify their compliance with the access restrictions. We are concerned that the vastly greater number of persons potentially having access under the proposal will result in a much greater potential for misuse.

Second, in recent years there have been significant advances in the types of technologies that can be used to effect re-identification, and there is more data today that can be obtained from various sources to assist in re-identification. Moreover, advances in technologies can be expected to continue, and the proliferation of data sources is likely to continue as well. For these reasons, the risk of re-identification is greater today compared to several years ago, and that risk is likely to increase. And the dividing line between "potentially sensitive" and less sensitive data fields is also likely to shift over time. While risk of re-identification for impermissible purposes can, to some extent, be mitigated through measures such as access restrictions (as described in section 4), these risks cannot be fully eliminated. Consequences of these risks could include reduced or eliminated offering activity by issuers or non-participation by investors (or investors simply not accessing the data).

We also wish to highlight that the risks and consequences of potential re-identification are exacerbated by the fact that the proposed revisions to Regulation AB contemplate asset level data not just at the time of issuance, but with each distribution on the asset-backed security which in most cases is monthly. Furthermore, the ongoing reporting for most asset types is required to provide loan level data for delinquencies and foreclosures, charge-offs and other actions. Potential identification of this extremely sensitive data to a specific individual is a very serious risk, and we request that consideration be given to changes in the ongoing reporting required content to address this concern.

With the uncertainty created by privacy law considerations, we anticipate that the process of commenting on the subject may give rise to a further and ongoing re-consideration by the industry of best practices around asset level data in light of the risk of re-identification. For residential mortgages, this might include consideration of whether specific data fields should be withheld or provided as ranges rather than exact numbers, dates or locations. Recognizing this can impact the provision of data that is considered absolutely necessary by issuers and investors alike, this potential reduction in disclosure could have significant negative consequences to the re-establishment of the private label RMBS market.

Accordingly, we respectfully request that as a gating issue for moving forward with the issuer website requirements under the staff memorandum together with the asset level data requirements under the proposed revisions to Regulation AB, the Commission should co-ordinate with the CFPB to assure that the CFPB implements a regulatory change or issues an authoritative interpretation under FCRA, to provide essential protections against liability as to the FCRA as outlined in section 2.b.

[30] We note that typical practice in classes of asset-backed securities offered pursuant to Rule 144A, is that the securities remain contractually restricted for the life of the transaction, even after they would become unrestricted for purposes of Rule 144.

4 Access restrictions and related issues

The proposed approach contemplates that the complete set of asset-level data required under revised Regulation AB would be provided through an issuer or issuer-sponsored website. Under this approach, "issuers could determine for themselves the specific controls needed for the dissemination of sensitive information" on a website, in a manner that would result in "appropriate safeguards to comply with privacy laws."

The proposal in effect "punts" to the issuer the issue of what controls are needed to comply with privacy laws. This is not inappropriate, because the Commission is not charged with responsibility for interpreting privacy laws, other than the GLBA. Yet aside from the issue of what controls are appropriate, this approach raises more fundamental questions that should be considered by the Commission. These questions include:

- Should the issuer have reasonable discretion to withhold specific disclosure items, or to restrict access to specified classes of investors and other market participants, as needed to minimize liability under privacy laws?
- Should the issuer or an investor be required to bear even a remote risk of privacy law liability? Should the issuer or an investor be required to bear reputational risk?
- What risks may be unintentionally imposed on investors?
- Would it be permissible as a securities law policy matter to restrict access to limited classes of investors, such as qualified institutional buyers, or investors that certify that they intend and have the ability to use the data to perform independent due diligence?

While it is premature at this time to have any certainty as to exactly what access restrictions an issuer would consider necessary to impose on an issuer-hosted asset level data website, our working hypothesis is that at a minimum, these restrictions might include some or all of the following:

- a signed user agreement covering the following items,
- agreement to use the data solely for investment purposes and not for any other purpose,
- prohibition on disclosure of the data to any other person for any unrelated purpose,
- certifications that the investor has adequate safeguards/controls in place (including encryption) to protect data from unauthorized internal and external parties, adequate safeguards/controls in place to dispose of the data properly, and adequate security breach protocols,
- an agreement to indemnify the issuer for any liability resulting from misuse by the investors and potential investors,
- representations as to the investor meeting specified criteria, and
- a requirement that users certify that they intend and have the ability to use the data to perform independent due diligence.

We note that in accordance with existing data safeguard regulations, privacy policies of financial institutions typically require a review of potential recipients of personally identifiable financial information, to ensure they have appropriate data safeguards in place. Here, given the sensitivity to the concern about the risk of persons using this data in combination with other available data to re-identify the borrower, it is likely that the restrictions would be similar to those which would be used if the data did include fields that directly identified the borrower. The access restrictions that we envision would not be satisfied with a click through screen or a boilerplate form agreement. As mentioned above, the more data points that are disclosed and the more granular the data is, the more robust data safeguard requirements need to be. We note also that this access granting process will be time consuming, expensive and cumbersome to both issuers and investors and if not completed prior to the offering process may preclude non-cleared investors from participating.

However, we do not intend that the access restrictions would impose on the user a duty of trust or confidence (see section 5 below).

It is essential that issuers have the ability to design the access restrictions, and that the rules do not set forth specific certifications that would be required in order for a user to gain access as was done with Rule 17g-5. At the same time, we are concerned about the difficulty that could be imposed on investors in having to navigate varying access restrictions across different issuers and asset classes. Even with these types of access restrictions, some of our issuer members believe that they would not want to make these disclosures out of concern for unpredictable privacy law liability and reputational risk. Some issuers are also concerned about investors which are associated, or on common computer systems, with lending institutions that are in the business of competing in the issuer's sectors, and whether the investor has internal controls in place to limit access only for investing purposes. (See also the discussion in section 2 d above.)

Investors are also concerned about the proposed approach. Investors do not want the liability risk that may be imposed by the access restrictions. Investors also do not want the liability risk and the reputational risk that may result from accessing the data, particularly if it is downloaded onto the investor's systems. Considering that access restrictions may have securities law implications, and given potential user liability around use and disposal of data, it is also essential that investors have input into the design of the access restrictions.

Investors are further concerned about the approach because it would require them to deal with each different issuer separately, and potentially to have to review and negotiate each issuer's unique form of user agreement and other access restrictions. Investors believe this will create a disincentive to using the issuers' websites to access data. Furthermore, in the context of a specific offering, the additional time needed to resolve these issues as a practical matter could preclude an investor from participating. Investors would strongly prefer a solution that provides "one stop shopping" to accessing this data, if the data is to be provided.

A potential result of these concerns is that investors could simply avoid investing in certain asset classes of ABS, or that the market for certain classes could be thin. We are concerned about the negative effects this would have on liquidity, and more broadly on the availability and cost of credit in the real economy. Further, there is the risk that borrowers may prefer to borrow from originators that do not use securitization as a source of funding, and who therefore would not have any need to make asset level data disclosures.

There is little point in building a system that imposes significant compliance burdens and expense on securitization market participants in order to achieve a policy objective if the intended users do not access the data, which would defeat the policy objective of achieving increased disclosure for investors. The proposed approach could result in an unjustified compliance burden and expense, create disincentive for investors to access the data or participate in a securitization transaction, or cause issuers to simply exit the securitization market or precluding new entrants.

Finally, while as stated above we cannot predict at this time the exact nature of access restrictions that would be imposed on an issuer website, our members do not foresee any circumstance under which access would be granted to investors or prospective investors who are individuals. We recommend that the policy implications be considered of regulations which could in practice result in different levels of disclosure to different classes of investors in a public offering.

For the reasons described above, we believe that asset level data as contemplated in the proposal should not be disclosed in a manner that results in broad, unrestricted dissemination, but rather can only be provided with access limitations and user agreements that are comparable to the ways in which this information is made available to sophisticated investors today. This necessarily means that, in a public offering, some investors or potential investors may not in practice have access to this data. In light of this, we request that the Commission add to the proposal a provision to the effect that, if a given investor is not able to access the asset level data due to reasonable and necessary restrictions of the types described above, that the issuer will not be liable for having omitted to make this disclosure to that investor.

We note that the issues identified above could be mitigated but not entirely eliminated, if a FCRA exemption is provided as described in section 2 above. As discussed above however, there would remain in any event reputational risks to originators, issuers and investors, as well as risks to borrowers.

5 <u>Duty of trust or confidence</u>

We also recommend that the proposal be reviewed carefully to make sure that restrictions imposed on investors in accessing the asset level data do not cause the data to be considered not "public" information, and do not inadvertently impose on investors a "duty of trust or confidence" that could prevent investors from trading the related securities.

As described above, we anticipate that any user gaining access to an issuer website for the provision of asset level data would be required to sign an agreement including nondisclosure and use covenants. However, we do not intend that such an arrangement would create a duty of trust or confidence that would impair the user’s ability to trade on the information, as that would obviously run directly counter to the purposes of the disclosure. Accordingly, we recommend that appropriate revisions be made to Rule 10b5-1 and 10b5-2 to make it clear that access restrictions as described above would not create a duty of trust or confidence, and would not be deemed to be an agreement to maintain information in confidence.

By the same token, a user gaining access under these access restrictions should not be considered to owe a duty of trust or confidence for purposes of Regulation FD. As a consequence of not having such a duty, Regulation FD may require public disclosure of the information posted on the issuer website, in the case of registered asset backed securities. Accordingly, we recommend that appropriate revisions be made to Regulation FD to make it clear that disclosure under an issuer website so restricted would be compliant. We note that a website subject to the access restrictions described above may not constitute “broad, non-exclusionary distribution” as contemplated in the definition of public disclosure in Rule 101(e)(2) in Regulation FD. We recommend a revision to this definition that would result in posting of the data on the issuer website being deemed to be public disclosure. (While the staff memorandum contemplates that the issuer website content would be deemed included in the prospectus and periodic reports for liability purposes, this does not cause the information to be actually filed or furnished on Form 8-K, or to be provided by a permitted means under Rule 100(b)(2)(iii)).

We also note that the proposed asset level data fields should be reviewed to ensure they do not contain information that may give rise to exposure under other laws (such as pricing information, relative to antitrust law).

6 Third Party Data Providers

As noted in footnote 2 of the staff memorandum, an issuer could provide the data through a website maintained by a third party. The memorandum also notes that "some asset-level data is available today through third-party providers… for a fee." We note that we are very supportive of this aspect of the proposal. Issuers should have the option to use third party agents (which may be a consumer reporting agency or a central website data aggregator) to make the data available and control access to the data. This option should not be limited to the use of a specified or mandated central website data aggregator.

This section briefly discusses some of the pros and cons of an approach where one or more third party data providers host the data for a number of issuers in one or more asset classes. Each issuer would have full discretion as to whether to contract with such a provider, or to use its own website. The provider could be an existing vendor, or a new company, or could be established as a "utility" designed and funded by industry participants.

This approach potentially offers investors some degree of "one stop shopping", that is, the ability to access information about a wide variety of issuers in a single location, without the need to enter into separate user agreements with each issuer. Some of our investor members have indicated that they would appreciate the streamlining and ease of access that could result.

We note, though, that this approach does not seem to offer any advantages regarding mitigation of privacy law liability or reputational risks. Unlike some current practices for similar vendors, because the data set uploaded from the issuer would include both credit information related to the origination of the loan as well as asset data that potentially is personally identifiable, vendors offering such a service would likely need the same exemptions under the FCRA and other laws (as outlined in section 2 above) as issuers would, in order to proceed.

These services are also subscription based and are costly to operate, so the question of who should bear the cost arises when considering this approach as a means of fulfilling Regulation AB disclosure requirements. Yet at the same time, the cost efficiencies gained by vendors supporting multiple issuers and investors reduces the total cost borne by the industry as a whole. Users, rather than issuers, in many cases pay the cost of these services today. In this context, if the rules permitted issuers to make Regulation AB required asset level data through a vendor, we anticipate the data would have to be provided to investors free of charge. Additionally, we would anticipate that the vendor could allow each participating issuer to set its own access restrictions and controls, which could undercut the advantages to investors of potentially streamlined access.

While the idea may have merit, unfortunately we believe that given the limited time frame for commenting on the proposal, there is not adequate time to develop views on the feasibility of such a third party approach. However, SFIG would welcome the opportunity to more fully vet this idea in the context of a partial re-proposal of the revisions to Regulation AB indicating what the final required data fields will be and requesting comment on the issuer website proposal and related privacy issues.

Finally, we note that some of the precedents cited in the staff memo for providing asset level data through websites are distinguishable from the proposed approach. With respect to CMBS offered in the United States, the underlying assets are not consumer loans, so the privacy laws and related concerns discussed above are not applicable. (Of course, there are other reasons why access to asset level data for CMBS should be restricted.) And with respect to the asset level data gathering procedures required by the Bank of England, issuers there are of course not subject to US privacy laws and the concerns discussed above.

7 Cross border implications

Additionally, several cross border issues must be considered. Privacy, consumer protection and securities laws vary across jurisdictions. In certain jurisdictions, local laws may not permit the proposed asset level disclosure in the manner suggested, creating significant problems for non-U.S. issuers of asset-backed securities in the U.S. Furthermore, many of the protections requested in this letter, including safe harbors, exceptions, and interpretive guidance in the context of U.S. laws, will not be available to non-U.S. issuers, borrowers or investors. The SEC's proposal acknowledges that issuers would need to rely on an exclusion from the FCRA (permitting disclosure to "potential investors") to share the proposed asset-level information without being in breach of the FCRA. We note that similar consumer protection laws exist in jurisdictions outside of the U.S. but may not include an exception for disclosure to potential investors. Accordingly, compliance with the proposed requirements could cause non-U.S. issuers of asset-backed securities to be in breach of their local laws and give rise to additional liability for them and their non-U.S. investors. In the case of cross-border registered offerings, the pool of investors and potential investors could include virtually anyone. In such an offering, information provided to U.S. investors generally would also be made available to its non-U.S. investors and potential investors. Individuals located in foreign jurisdictions may not be subject to U.S. laws if they are accessing data kept on computer systems located outside the U.S. Furthermore, individuals located in jurisdictions without an extradition treaty with the U.S. could access the data (regardless of where located) and potentially be beyond the reach of U.S. laws and the laws of the issuer's or borrower's jurisdiction. There is a risk, therefore, that borrowers' information could be used improperly with potentially no recourse against the person misusing the information.

Particularly for foreign issuers that may not have the benefit of any exemptions that could be instituted in the U.S. to facilitate the new requirements, issuers/originators may need to spend significant resources amending their standard agreements with borrowers/consumers to include consents that are broad enough and specific enough to facilitate compliance with the new requirements. This could potentially sideline issuers for months or even years in some cases waiting for a large enough book of assets with such consent features to be able to reconstitute their asset pool.

We also note that the ability to identify borrowers from disclosed data will vary from country to country based on the characteristics of the country and the specific data fields as implemented with respect to that country. For example, a postal code in some countries may include a very small slice of the population or be for a single building which would increase the possibility of re-identification. Finally, while not opining on the appropriateness of the potential disclosure requirements, we would also note that data fields captured in the ordinary course of originations outside the U.S. may differ substantially from the asset level data fields that will be required under Regulation AB.

8 Costs and burdens

We respectfully submit that there are many potential costs to the issuer website proposal that are not reflected in the discussion included in the staff memorandum. These costs include:

- Audit (internal and external) and data verification requirements
- Legal counsel review (user agreements, non-disclosure agreements, other certifications and undertakings, and privacy law compliance)
- Staff to administer access restrictions and controls, including to determine investor eligibility
- Additional compliance staff
- Additional technical support (for example, ordinary maintenance such as resetting passwords for users)

In addition to costs related directly to the development and maintenance of issuer websites, we would like to note other costs associated with this proposal, including but not limited to:

- Costs of renegotiating contracts with information providers, originators of financial consumer assets usually have contracts with all the national credit bureaus to receive credit bureau information, including credit scores, in their origination process. These contracts typically contain restrictions on the ability to further disclose.
- Costs of revising borrower facing privacy policies and disclosures.
- Systems and hardware.

In light of the fact that the proposed approach was conveyed by a staff memorandum, rather than a formal re-proposal, it appears to us that a formal and complete cost benefit analysis is yet to be provided.

Some of the most significant variable costs that would be incurred by issuers in complying with the proposed requirements would be audit and data verification tasks performed for the ongoing, periodic data reports that would be created for each distribution on the ABS. Because of the sensitive nature of the data that would be required to be disclosed, significant resources (including, potentially, full-time employees) would need to be allocated on a near-constant basis to ensure the accuracy of each data file. These costs, while large for all issuers, could be especially burdensome on smaller issuers who depend on access to the ABS markets to fund their businesses.

Based on its experience with its other outward facing websites, one large and frequent ABS issuer, estimates that building a website with access controls for hosting loan level data would cost approximately $150,000. Ongoing administration and maintenance for the site would cost approximately $250,000 per year and would include maintaining auditable controls, records retention and data management. In addition, to these direct costs, this issuer anticipates significant legal costs associated with this project, including for developing a user agreement, terms and conditions and a confidentiality agreement, expanding data safeguarding policies and procedures, and revising privacy notices. It is difficult to make these cost estimates given that we do not know the specifics of the final Regulation AB revisions for loan level data requirements and given that the scope of these agreements and policies may depend on the nature and number of data fields required to be provided.

Based on its experience in implementing the loan level data requirements for European Central Bank eligibility, this issuer estimates costs for systems modifications to create and format the data for posting to the website would cost approximately $600,000 and take approximately 18 months to complete.

Given the significant technological and contractual requirements around developing the proposed websites, we would recommend an 18 month period from publication of the final revisions to Regulation AB, to its compliance date.

Finally, we object to the portion of the proposal that contemplates that the data fields that are not "potentially sensitive" would be filed on EDGAR. We believe this filing would be at the same time both substantially redundant, imposing wholly unnecessary costs on the issuer, as well as materially incomplete, because it would omit data fields that Regulation AB requires to be provided to investors.

****

We appreciate the opportunity to comment on the proposed approach. Please contact the undersigned at Richard.Johns@sfindustry.org or 202-524-6301 with any questions or comments.

Sincerely,

Richard Johns
Executive Director