STRUCTURED FINANCE ASSOCIATION

May 9, 2022

By E-Mail: ***rule-comments@sec.gov***

Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090
Attn: Vanessa A. Countryman, Secretary

Re: Release Nos. 33-11038; 34-94382; IC-34529 (File No. S7-09-22)

Ladies and Gentlemen:

The Structured Finance Association ("SFA")[1] appreciates the opportunity to submit this letter in response to the request of the Securities and Exchange Commission (the "Commission") for comments regarding Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22, dated March 9, 2022 (the "Proposing Release"),[2] relating to the proposal of rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 (the "Exchange Act").

We appreciate and are supportive of the Commission's goal to enhance and standardize disclosures regarding cybersecurity matters by public companies and believe that registrants and investors would benefit from further guidance on this subject. At the same time, in its current form, the proposed disclosure framework is focused almost exclusively on corporate issuers that have operations and businesses, rather than on asset-backed issuers that have no such operations or businesses and, as a result, it is not possible to apply the proposed reporting framework to asset-backed issuers without significant revisions and clarifications first.

There is nothing in the proposed rules to suggest that, in the context of asset-backed securities ("ABS") transactions, they would apply to transaction parties other than the asset-

[1] SFA is a member-based trade industry advocacy group focused on improving and strengthening the broader structured finance and securitization market to help its members and public policy makers responsibly grow credit availability for consumers and business across all communities. With over 360 members, SFA represents all stakeholders in the securitization market, including consumer and commercial lenders, institutional investors, financial intermediaries, law firms, accounting firms, technology firms, rating agencies, servicers, and trustees. SFA was established with the core mission of supporting a robust and liquid securitization market, recognizing that securitization is an essential source of core funding for the real economy. As part of that core mission, SFA is dedicated to furthering public understanding among members, policy makers, consumer and business advocacy groups, and other constituencies about structured finance, securitization, and related capital markets. Further information can be found at www.structuredfinance.org.

[2] "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," 87 Fed. Reg. 16590 (Mar. 23, 2022).

backed issuer, and we believe the proposed rules are far too extensive for a party performing activities that support the transaction in one way or another, but where that transaction party is neither the issuer of, nor an obligor on, the ABS. We also believe there are meaningful differences between the potential impact of cybersecurity risks and incidents on investors in corporate securities versus ABS. The primary area of potential cybersecurity risk to an ABS transaction relates to the breach of information systems used by a servicer, including the breach of personal information maintained on those information systems, which, depending on the facts and circumstances, could disrupt servicing of the underlying pool assets.

In light of these differences, we believe the focus of any proposed cybersecurity disclosure rules for ABS transactions should be on servicers, whose roles in ABS transactions are generally more significant than the roles of other transaction parties and whose cybersecurity vulnerabilities are more likely to be relevant to ABS investors. We urge the Commission to propose rules for asset-backed issuers that are better aligned with the disclosure and reporting framework established under Regulation AB and to provide the ABS market with opportunity for public comment on any such proposed rules.

I. Background

As noted by the Commission, there are no disclosure requirements in Regulation S-K or S-X that explicitly refer to cybersecurity risks or incidents. This is also the case for Regulation AB. Over the past decade, the Commission and its staff (the "Staff") have issued interpretive guidance concerning the application of existing disclosure and other requirements under the federal securities laws to cybersecurity risks and incidents.

In 2011, the Staff of the Division of Corporation Finance issued interpretive guidance (the "2011 Staff Guidance"), providing the Division's views concerning operating companies' disclosure obligations relating to cybersecurity risks and incidents. In 2018, the Commission issued additional interpretive guidance (the "2018 Interpretive Release" and, together with the 2011 Staff Guidance, the "Commission Interpretive Guidance"), reinforcing and expanding upon the 2011 Staff Guidance to assist operating companies in determining when these disclosure obligations may arise under existing disclosure rules.

While the Commission Interpretive Guidance addressed these disclosure obligations for operating companies, asset-backed issuers have adapted that guidance to their transactions when assessing the materiality of cybersecurity risks and incidents in the course of preparing disclosure required in registration statements and prospectuses under the Securities Act of 1933 (the "Securities Act"). Many asset-backed issuers include enhanced disclosure relating to cybersecurity risks and incidents, based on general principles of materiality as applied in the context of an ABS transaction. While these disclosures vary in their level of detail, they are typically presented as risk factors in the prospectus and address, among other things, how

cybersecurity risks and incidents may disrupt the servicing and performance of the pool assets.[3] In cases where the servicer has experienced a cybersecurity incident, depending on all of the facts and circumstances, the incident may also be disclosed, either in a cybersecurity risk factor or elsewhere in the prospectus, such as in the discussion of the servicer's servicing practices. Depending on the materiality of a cybersecurity incident, this disclosure may address the cause, scope, and impact of the incident, as well as remedial steps the servicer has taken or is taking in response to the incident.

II. Application of Proposed Cybersecurity Reporting Framework to Asset-Backed Issuers

A. The Proposed Framework Does Not Take into Account Key Aspects of ABS Transactions That Differentiate Them from Corporate Securities Transactions

On its face, the proposed rules apply to "registrants" and would, therefore, apply to corporate issuers and asset-backed issuers alike, though the proposed rules would include an exception for a narrow subset of these disclosures relating to certain governance matters in cases where the asset-backed issuer does not have any executive officers or directors.

The proposed reporting framework does not, however, appear to have been fully fleshed out for asset-backed issuers. For example, under Regulation AB, the term "asset-backed issuer" is defined as "[t]he depositor for the asset-backed securities acting solely in its capacity as depositor to the issuing entity."[4] The depositor is, however, often a special purpose vehicle whose activities are typically limited to receiving or purchasing and transferring or selling the pool assets to the issuing entity in connection with one or more securitization transactions. As the depositor neither holds the pool assets nor issues the ABS supported by that asset pool, it would seem that the Commission may have intended the focus of its proposed disclosure rules to be on the issuing entity rather than on the asset-backed issuer.[5]

Even if the Commission did intend to apply its proposed disclosure rules to the issuing entity, that entity is also typically a newly-formed special purpose vehicle whose activities are limited to "passively owning or holding the pool of [self-liquidating financial] assets, issuing the

[3] In some cases, where a servicer is an affiliate of the asset-backed issuer and is itself a reporting entity (or the subsidiary of a reporting entity), an asset-backed issuer may include some disclosures regarding its affiliated servicer's cybersecurity risk management.

[4] *See* Item 1101(b) of Regulation AB, Rule 191 under the Securities Act, and Rule 3b-19 under the Exchange Act.

[5] We note General Instruction J to Form 10-K, which provides guidance on use of the Form by asset-backed issuers and identifies information that may be omitted from the Form and substitute information that is to be included. General Instruction J.(1)(m) provides: "If the *issuing entity* does not have any executive officers or directors, Item 10, Directors and Executive Officers of the Registrant, Item 11, Executive Compensation, Item 12, Security Ownership of Certain Beneficial Owners and Management, and Item 13, Certain Relationships and Related Transactions," the registrant may omit the information called for by those Items. [Emphasis added.]

asset-backed securities supported or serviced by those assets, and other activities reasonably incidental thereto."[6] As a passive special purpose vehicle with no operations or business, the proposed disclosure rules would not seem to be any more relevant to the issuing entity than they would be to the depositor.[7]

The proposed rule and form changes are also focused almost exclusively on corporate issuers that have operations and businesses, rather than on asset-backed issuers that have no such operations or businesses. For example, the proposed rules –

- Define "cybersecurity incident" as "an unauthorized occurrence on or conducted through a *registrant's* information systems that jeopardizes the confidentiality, integrity, or availability of a *registrant's* information systems or any information residing therein" [emphasis added];

- Define "information systems" by reference to "information resources, *owned or used by the registrant*" [emphasis added];

- Provide for certain disclosures about the issuer's cybersecurity risk management, strategy, and governance, such as disclosing the role cybersecurity plays in a company's strategy, financial planning, and capital allocation; and

- Require that the issuer's periodic filings reflect any "material changes, additions, or updates" to previously-reported cybersecurity incidents.

As limited purpose or passive special purpose vehicles with limited activities and no operations or businesses, asset-backed issuers and issuing entities do not own or use information systems. Consequently, cybersecurity risk management, strategy, and governance are not relevant to these entities and the rules, as proposed, would not produce meaningful information to investors.

In addition, to effectuate the proposed requirement that the issuer's periodic filings reflect any material changes, additions or updates to previously-reported cybersecurity incidents, the Commission is proposing conforming changes only to Forms 10-K and 10 Q, not to Form 10-D. It is not possible, therefore, to apply the proposed reporting framework to asset-backed issuers without significant revision and clarification first.

[6] *See* Item 1101(c)(2)(ii) of Regulation AB.

[7] As the Commission is aware, because the issuing entity is a passive special purpose vehicle with no operations or business, Regulation AB does not require the issuing entity to comply with the requirements of Item 101 of Regulation S-K (Description of Business), Item 407 of Regulation S-K (Corporate Governance) or Item 303 of Regulation S-K (Management's Discussion and Analysis of Financial Condition and Results of Operations. In addition, Regulation AB does not require audited financial statements for the issuing entity in either Securities Act or Exchange Act filings.

There is nothing in the proposed rules to suggest that they would apply to transaction parties other than the asset-backed issuer or issuing entity and we do not believe it would be appropriate to apply the proposed cybersecurity reporting framework in its current form to such parties. As the Commission is aware, Regulation AB identifies transaction parties that perform various activities related to the ABS transaction, including the ABS sponsor, depositor, issuing entity, servicer, originator, and trustee. Transaction parties support an ABS securitization transaction in different ways, with some whose role is of a narrower scope (such as a trustee) and others whose role generally is of a broader scope (such as a servicer). Some ABS transactions have one servicer while others have multiple servicers or a master servicer and one or more primary servicers or a backup servicer. A servicer may service the entire asset pool or only a portion of the pool. Even among servicers, therefore, they can support an ABS securitization transaction in different ways, some of a broader scope and others of a narrower scope. Servicers may or may not be affiliates of the ABS sponsor, depositor, issuing entity, or one another.

Aside from the depositor, transaction parties are not the issuer of the ABS. They are engaged to perform a designated role with specified duties, they are generally subject to removal for cause, and, while they perform activities that support the transaction in one way or another, they are not an obligor on the ABS. It is extraordinarily unlikely that a transaction party's financial performance or position would be impacted by a cybersecurity incident to such an extent as to impede its ability to perform its duties and responsibilities to the securitization transaction. In the ordinary course, therefore, the financial performance or position of a transaction party is not material to the ABS transaction and Regulation AB does not require information on the financial condition of a transaction party under those circumstances.[8] Cybersecurity risks and incidents may disrupt certain activities performed by a transaction party and, as indicated previously, many asset-backed issuers currently disclose this risk. However, this risk does not rise to the level that an asset-backed issuer should be required to comply with the Commission's proposed cybersecurity reporting framework.

Harmonizing Regulations is of Critical Importance

Finally, any Commission proposal affecting transaction parties would need to be carefully harmonized with the cybersecurity risk and incident disclosure rules and regulations by which many transaction parties must already abide. Regulated financial institutions are subject to other rules and regulations concerning cybersecurity risk and incident disclosure. For example, banks and bank service providers are subject to the Cyber-Security Incident Notification final rule published in November 2021 by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Board of Governors of the Federal Reserve System.[9]

[8] For example, Regulation AB does not require information regarding a servicer's financial condition unless there is a material risk that its financial condition could have a material impact on pool performance or performance of the ABS. *See* Item 1108(b)(4) of Regulation AB.

[9] *See* 12 C.F.R. Part 53, §53.1 *et seq*.

Cybersecurity Disclosure Framework for ABS Demands Tailored Standards Aligned with Regulation AB

Taking all of this into account, we believe a cybersecurity reporting framework developed for issuers is far too extensive for a party performing activities that support the transaction in one way or another, but where that transaction party is neither the issuer of, nor an obligor on, the ABS. Simply put, while a transaction party may have an important role in a securitization, it is qualitatively different from an issuer's role in a corporate securities transaction, and we believe it would be inappropriate to equate the role of any such transaction party with that of an issuer in a corporate securities transaction or, therefore, to apply the same cybersecurity reporting framework to securitization transaction parties as the Commission is proposing to apply to corporate issuers.

We believe our views are also borne out by the existing disclosure standards set forth in Regulation AB, which recognize that the transaction parties have a material role in the ABS transaction but also tailor and limit those disclosure requirements to the capacity in which that party is acting.[10] Notably and appropriately, these disclosure requirements do not bear any relationship to the scope and extent of disclosure required of corporate issuers.

The Regulation AB disclosure and reporting regime is also not an "integrated" regime, meaning that the disclosure standards that apply to Securities Act filings and the reporting standards that apply to Exchange Act reports are almost entirely different and distinct, with virtually no overlap. ABS disclosure in registration forms and prospectuses includes transaction party disclosure while ABS reporting periodic reports does not; instead relating primarily to the reporting of current pool performance and distribution information on the ABS.

If the Commission sought to apply the proposed cybersecurity reporting framework in its current form to one or more of these transaction parties, it would, therefore, represent an extraordinary departure from, and seismic expansion of, the existing disclosure and reporting standards under Regulation AB. We respectfully submit that any departure from the existing disclosure and reporting standards under Regulation AB should be the subject of proposed rulemaking focused on ABS with an opportunity for robust public comment to identify and assess the competing considerations bearing on those disclosure and reporting proposals, including the relative costs and benefits of such proposals.

B. Incident Reporting

As noted above, as part of the proposed cybersecurity reporting framework, the proposed rules would require the registrant to disclose a cybersecurity incident within four business days

[10] Regulation AB requires an asset-backed issuer to disclose the background and experience of various transaction parties, the nature of their duties and responsibilities under the transaction documents, and certain other targeted matters only when and if they arise, such as the disclosure of any material legal proceedings and the existence of any affiliations, relationships and related transactions.

after the registrant determines that it has experienced a material cybersecurity incident, pursuant to proposed new Item 1.05 to Form 8-K. The Commission is proposing to include an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

If the Commission sought to expand this reporting requirement to cover cybersecurity incidents experienced by another transaction party identified under Regulation AB, asset-backed issuers would have several concerns:

First, any such proposal would significantly increase the reporting burden on asset-backed issuers as compared with corporate issuers because asset-backed issuers would have to attempt to build out policies and procedures to determine whether another transaction party, possibly an unaffiliated party, had experienced a cybersecurity incident, as well as whether the incident was material to the ABS securitization.

Second, asset-backed issuers believe it is extremely unlikely that an unaffiliated party would be willing or able to share information about the occurrence of a cybersecurity incident within a timeframe that would meet the proposed filing requirement.[11] And, even then, asset-backed issuers think the unaffiliated party would be willing or able to disclose only a minimum amount of information about the incident.

Third, assuming the parties were able to move beyond the challenges identified in the preceding paragraphs, the determination of whether a cybersecurity incident experienced by another transaction party was material to the ABS securitization transaction could be difficult to ascertain, particularly if the party experiencing the incident were unwilling or unable to share sufficient information about the nature of the incident to make a materiality determination.

We once again respectfully submit, therefore, that any departure from the existing reporting standards under Regulation AB should be the subject of proposed rulemaking focused on ABS with an opportunity for public comment to identify and assess the competing considerations bearing on those reporting proposals. By way of example only, if the Commission were to propose a reporting requirement for cybersecurity incidents experienced by another transaction party, in addition to addressing the practical challenges outlined above, we believe any such reporting requirement should be qualified to the extent that any information called for regarding the incident is not determined by, or is unavailable to, the asset-backed issuer.[12]

[11] To the contrary, asset-backed issuers think it is far more likely that an unaffiliated party would be compelled to delay notifying the asset-backed issuer of the incident for some period of time for any number of reasons, including to allow adequate time for the unaffiliated party to assess the nature of the incident and make its own materiality determination, and then to obtain the necessary approvals to notify the asset-backed issuer of the incident.

[12] The Commission adopted such a qualified reporting requirement with respect to Item 6.02 to Form 8-K (Change of Servicer or Trustee). *See* Instruction to Item 6.02, which provides:

C. Access to Shelf Registration

The Commission's proposed cybersecurity periodic reporting framework would also include certain corresponding changes to the Exchange Act reporting registrant requirements in Form SF-3. As the Commission knows, these requirements generally require that the depositor and certain affiliates of the depositor be current and timely in their Exchange Act reporting requirements during a 12-month look-back period immediately preceding the filing of the registration statement. The requirements currently exclude the reporting of certain reportable events on Form 8-K from the timely reporting requirement, but continue to require that these depositors be current in their reporting requirements. These registrant requirements also require that these depositors' other periodic reports (e.g., on Forms 10-D and 10-K) be both current and timely. Finally, these registrant requirements also apply at the time of the depositor-registrant's annual compliance evaluation under Form SF-3, to determine whether the depositor-registrant remains eligible to conduct further takedowns from its effective Form SF-3 registration statement.

If the Commission sought to apply all or any part of the proposed cybersecurity reporting framework to one or another transaction party identified under Regulation AB, the depositor-registrant's access to shelf registration – both at the time a Form SF-3 registration statement is initially filed and at the time of its annual compliance evaluation for continued access to an effective Form SF-3 registration statement – could depend on whether one or another unaffiliated transaction party provided required cybersecurity disclosures in a timely manner. **We respectfully submit that a loss of access to shelf registration due to circumstances entirely outside the control of the asset-backed issuer would be punitive in nature and unlike any potential consequence a corporate issuer would face under the proposed cybersecurity reporting framework.** This is another significant reason why the Commission should not proceed to adopt rules applying the proposed cybersecurity reporting framework to asset-backed issuers without proposing rules in this area focused specifically on ABS.

D. Any Rulemaking Should Apply Prospectively

Any Commission rulemaking that impacts asset-backed issuers must distinguish between asset-backed issuers whose reporting obligations arose by virtue of ABS that were issued prior to the compliance date(s) for any such new rules ("legacy ABS"), as compared with asset-backed issuers whose reporting obligations will arise by virtue of ABS that will be issued after any such compliance date(s).[13] Thousands of registered legacy ABS issuances, each by a separate asset-backed issuer, have been completed over a period of many years and are currently outstanding. These asset-backed issuers completed those legacy ABS issuances on the basis of a regulatory

"To the extent that any information called for by this Item regarding such servicer or trustee is not determined or is unavailable at the time of the required filing, the registrant shall include a statement to this effect in the filing and then must file an amendment to its Form 8-K filing under this Item 6.02 containing such information within four business days after the information is determined or becomes available."

[13] This distinction between legacy ABS and newly-issued ABS applies equally to asset-backed issuers that are amortizing trusts or revolving master trusts.

framework that did not include cybersecurity reporting requirements. For the vast majority of these issuances, the related transaction documents do not contain provisions that would support reporting in accordance with a prescribed cybersecurity reporting framework, or that would provide for the funds necessary to cover the costs of reporting in such a manner. **It is imperative, therefore, that any Commission rulemaking that proposes cybersecurity reporting requirements for asset-backed issuers exclude legacy ABS from these additional reporting requirements.**

E. Inline XBRL Would Raise Compliance Implementation Costs While ABS Investors Don't Use It

The Commission is proposing to require registrants to tag the information specified by Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K in Inline eXtensible Business Reporting Language (Inline XBRL) in accordance with Rule 405 of Regulation S-T.[14] If asset-backed issuers were excluded from the proposed tagging requirements, they would submit any required cybersecurity disclosures in unstructured HTML or ASCII.

As the Commission notes, asset-backed issuers are not subject to Inline XBRL requirements in Commission filings and would incur initial Inline XBRL compliance implementation costs, such as the cost of training in-house staff to prepare filings in Inline XBRL and the cost to license Inline XBRL filing preparation software from vendors. Some asset-backed issuers are, but many others are not, affiliated with registrants that are subject to Inline XBRL requirements. For those asset-backed issuers that have such affiliates, we do not believe the asset-backed issuers would be able to leverage those affiliates' existing Inline XBRL tagging experience and software in a manner that would significantly mitigate these initial Inline XBRL implementation costs. For those asset-backed issuers that have no such affiliates, the initial compliance implementation costs will likely be even higher.

Given the nature of our comment, questions, and concerns regarding the proposed rules, it is difficult to fully assess the Commission's proposal to require the cybersecurity disclosures to be presented in Inline XBRL. Similarly, in light of our comments, we believe any rules the Commission proposes for ABS must first be better aligned with the disclosure and reporting framework established under Regulation AB. **Notably, however, ABS investors do not use (or seek to use) Inline XBRL in connection with their review of ABS disclosure and, as such, we believe the perceived benefits of such tagging in the ABS market would be negligible and would be far outweighed by the costs that asset-backed issuers would incur.**

[14] The Commission indicates that an Inline XBRL requirement would allow investors to extract and search for disclosures about cybersecurity incidents reported on Form 8-K, updated information about cybersecurity incidents reported in a registrant's periodic reports, a registrant's cybersecurity policies and procedures, management's role in assessing and managing cybersecurity risks, and the board of directors' oversight of cybersecurity risk and cybersecurity expertise rather than having to manually run searches for these disclosures through entire documents.

III. Certain Considerations in Proposing Cybersecurity Disclosure Rules for Asset-Backed Issuers

As indicated above, there are a number of threshold issues with applying the proposed cybersecurity reporting framework to asset-backed issuers because the framework does not take into account key aspects of ABS transactions that differentiate them from corporate securities transactions. If the Commission seeks to adopt cybersecurity disclosure rules for ABS transactions, we urge the Commission to propose rules that are better aligned with the disclosure and reporting framework established under Regulation AB and to provide the ABS market with opportunity for public comment on any such proposed rules. We urge the Commission to consider the following in formulating any such proposed rules:

Cybersecurity Disclosure for ABS Transactions Should Focus on Servicers: We believe there are meaningful differences between the potential impact of cybersecurity risks and incidents on investors in corporate securities versus ABS and that the primary area of potential cybersecurity risk to an ABS transaction relates to the breach of information systems used by a servicer, including the breach of personal information maintained on those information systems, which, depending on the facts and circumstances, could disrupt servicing of the pool assets. We believe, therefore, that the focus of any proposed cybersecurity disclosure rules for ABS transactions should be on servicers, whose roles in ABS transactions are generally more significant than the roles of other transaction parties and whose cybersecurity vulnerabilities are more likely to be relevant to ABS investors.

Among Servicers, Cybersecurity Disclosure Should Focus on Primary Servicers and Should be Principles Based: As described earlier in this letter, some ABS transactions have one servicer while others have multiple servicers or a master servicer and one or more primary servicers or a backup servicer. A servicer may service the entire asset pool or only a portion of the pool. Servicers may or may not be affiliates of the ABS sponsor, depositor, issuing entity, or one another. A servicer's role may be broader in scope and include responsibility for management or collection of the pool assets and making allocations or distributions to holders of the ABS, or may be considerably narrower in scope and include only a specific aspect of the servicing function, such as that of a master servicer that may aggregate collections on the pool assets from one or more primary servicers or, alternatively, provide oversight of those activities by the primary servicer(s), in which case the master servicer has no responsibility for management or collection of the pool assets and instead simply monitors the primary servicers and maintains reports to investors that include information on pool performance and distribution information on the ABS.[15]

[15] In some cases, such as in repackaging transactions where the asset pool may be comprised of a single bond issued by an underlying corporate, municipal, or other obligor, there may be one transaction party, such as a trustee, whose role is extraordinarily narrow and involves serving as a passive recipient for distributions on the underlying bond and allocating and distributing the same to the ABS investors. In these cases, the transaction party may technically be a "servicer" as defined in Regulation AB, but the servicing function entails little more than that of a paying agent for the ABS.

Given this variability in the nature and scope of servicing across ABS transactions, we believe any proposed cybersecurity disclosure rules should apply only to primary servicers[16] and should be principles-based, to allow asset-backed issuers to adapt the disclosure standards to the context of their particular transaction structure. Any proposed rule should explicitly indicate that the level of disclosure will depend on, among other things, the nature and scope of the servicer's servicing activities in the ABS transaction.

Cybersecurity Disclosure Should Focus on Material Risks and Risk Management and Should Apply to Securities Act Disclosure Documents: Any proposed rules for ABS transactions should focus on material cybersecurity risks and related risk management, based on principles of materiality as applied in the context of an ABS transaction, but should not extend to matters of cybersecurity strategy or governance. In their current form, the proposed rules are far too extensive for a servicer, which performs activities that support the transaction but is neither the issuer of, nor an obligor on, the ABS.

The focus should also be on disclosure contained in Securities Act registration statements and prospectuses, rather than in ongoing Exchange Act reports. As indicated above, unlike the disclosure and reporting framework for corporate issuers, Regulation AB is not an integrated disclosure and reporting framework. It would simply be too significant of a departure from the existing framework, and too burdensome on asset-backed issuers, to impose ongoing reporting requirements relating to the cybersecurity readiness of any transaction party, including servicers.

Cybersecurity Incident Reporting: If the Commission were to propose a reporting requirement for cybersecurity incidents in ABS transactions, the focus should be on the same category of servicers as outlined above for Securities Act disclosure and the reporting rule should once again be principles based, to allow asset-backed issuers to adapt the reporting standard to the context of their particular transaction structure. Equally important, however, any proposed rules for incident reporting must take into account the practical challenges faced by asset-backed issuers, as outlined in Section II.B. above, and the implications of any such reporting requirement on asset-backed issuers' ongoing access to shelf registration, as outlined in Section II.C. above.

In cases where a servicer is not an affiliate of the sponsor, depositor or issuing entity, we believe a necessary, but not sufficient, element of any solution to these challenges would be to qualify such reporting requirement to the extent that any information called for regarding the incident is not determined by, or is unavailable to, the asset-backed issuer. We also believe any information disclosed in such cases should be qualified by the knowledge of the registrant. In addition, in cases where information about a servicer's cybersecurity incident is required in an asset-backed issuer's Exchange Act report and the servicer is itself a reporting entity (or a consolidated subsidiary of a reporting entity), we believe the Commission should provide a

[16] As the Commission is aware, Regulation AB currently draws distinctions in the level of disclosure required depending on whether the servicer services less than 10%, between 10% and 20%, or 20% or more of the pool assets. Regulation AB requires considerably less disclosure for servicers that service less than 20% of the pool assets.

mechanism whereby, in lieu of including such information, the asset-backed issuer is permitted to refer to the Exchange Act reports of the servicer (or its reporting parent company).[17]

Legacy ABS Should Be Excluded from Additional Cybersecurity Reporting Requirements: As indicated in Section II.D. above, it is imperative that any Commission rulemaking that proposes cybersecurity reporting requirements for asset-backed issuers exclude legacy ABS from these additional reporting requirements.

Transition Period: Asset-backed issuers will need time to build out processes by which to prepare enhanced cybersecurity disclosure in Securities Act registration statements and prospectuses, as well as to establish policies and procedures to determine whether an unaffiliated servicer has experienced a material cybersecurity incident. We will be able to formulate a more accurate assessment of the time that will be required upon reviewing proposed rules focused on ABS transactions. Preliminarily, assuming the Commission were to propose and, ultimately, adopt rules for ABS transactions that align with our comment letter, we believe asset-backed issuers would need a transition period of at least six months after the effective date for any such rules in their final form before they could comply.

* * * * *

SFA very much appreciates the opportunity to provide the foregoing comments in response to the Commission's Proposing Release. Should you have any questions or desire any clarification concerning the matters addressed in this letter, please do not hesitate to contact Kristi Leo, President via telephone at 917.415.8999 or via email at kristi.leo@structuredfinance.org or Jen Earyes, Head of Policy, 202.524.6302, jen.earyes@structuredfinance.org.

Sincerely,

Kristi Leo
President
Structured Finance Association

[17] The Commission has a similar mechanism for the presentation of certain other third-party information. *See* Item 1100(c) of Regulation AB.