Comments of World Privacy Forum
To the
Securities and Exchange Commission regarding Disclosure of Asset-Level Data
(Commission File No. S7-08-10)

Via email

Ms. Elizabeth M. Murphy, Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

April 18, 2014

The World Privacy Forum appreciates the opportunity to comment on the Memorandum from the Division of Corporation Finance regarding Disclosure of Asset-Level Data (Commission File No. S7-08-10), http://www.sec.gov/comments/s7-08-10/s70810-258.pdf. We are grateful for the re-opening of the comment period for asset-backed securities release, http://www.sec.gov/comments/s7-08-10/s70810.shtml.

I. Comment Background

In August 2012, we filed comments on the Notice of Proposed Rulemaking on Asset-Backed Securities, File Number S7-08-10. Our comments for that proposal are available at http://www.worldprivacyforum.org/2010/08/comments-wpf-files-comments-on-deeply-flawed-sec-plan-2/ and http://www.sec.gov/comments/s7-08-10/s70810-91.pdf. The World Privacy Forum and other public interest groups that signed the comments strongly opposed the original proposal.

We reproduce here the executive summary of those comments for ease of reference and to underscore what we see as the stakes in this matter. Our earlier comments emphasized the threat to personal privacy that the original proposal entailed, as well as the secondary consequences for security systems in use elsewhere and the unwelcome effect on the stability of asset-level instruments themselves.

"While we understand the purpose of and motivation for the Commission's proposed rule, the proposal is a direct and substantial threat to the privacy of every individual who obtains a mortgage. If adopted, the proposal would be an unprecedented release of individual-level financial data and would greatly increase borrowers' risk for identity theft and other problems related to the public release of detailed financial information. Specifically, the SEC's proposed rule would:

- Expand the risk of identity theft for every borrower whose information would be disclosed because of the rule;
- Place on the public record and online the largest amount of personal financial information about borrowers ever disclosed, including information never before made public;
- Circumvent or undermine privacy protections in other laws, including the Fair Credit Reporting Act, Health Insurance Portability and Accountability Act, and the Privacy Act of 1974;
- Weaken the utility and security of knowledge-based authentication techniques and activities by exposing details of mortgages to more people throughout the world and would undermine NIST electronic authentication recommendations;
- Undermine the financial stability of households;
- Threaten the stability of the asset-backed instruments that the proposed rule seeks to protect by placing all borrowers at greater risk to be victims of criminal activity and thereby lowering the value of the asset-backed instruments."[1]

We observe that the consumer data environment – the amount of data about consumers and the number of industry players that traffic in consumer data – continues to grow and will expand even more in the future. The demand for consumer data is already immense, and some in industry will pounce on any available data to add to their profiles, databases, and analytics. The concerns that we expressed in earlier comments about the use and misuse of consumer data have not diminished in any way. If anything, our concerns have grown stronger.

II. Comments and Concerns Regarding New Proposal

The new proposal, while far from perfect, does a better job of balancing the Commission's interest in disclosure with the privacy interests of borrowers. We do not endorse the proposal wholeheartedly, but we think it offers an outline of an approach that will do a better (but not perfect) job of protecting the privacy and other interest of consumers *with some adjustments*.

Key elements of the Division of Corporations Finance's new proposal are:

[1] <http://www.sec.gov/comments/s7-08-10/s70810-91.pdf. >.

- Relying on issuers to provide information to investors and potential investors through a Web site without disseminating the potentially sensitive information on EDGAR

- Use of an issuer or issuer-sponsored Web site that would permit issuers to implement their own procedures that would provide both flexibility and the possibility of innovation in the delivery of information and the design of privacy controls.

- Issuers would provide access to potentially sensitive asset-level data to investors and potential investors and would be permitted to restrict access as necessary to comply with privacy laws.

We would be happier with this proposal if it were practical to keep all sensitive asset-level data under the direct control of the Commission or, perhaps, the Consumer Finance Protection Bureau. Direct involvement by a federal agency, while no guarantee of a better outcome for data subjects, would provide better and clearer accountability for maintenance of the data as well as the possibility of meaningful enforcement.

A. Concern: Lack of Direct Control/Involvement by a Federal Agency

We regret the Commission's reluctance to accept responsibility here, and we ask that the Commission reconsider whether it would do a better and *more efficient* job than imposing a duty on a potentially large number of entities that have no experience protecting consumer data.

If the Commission is unwilling to do more, it should be prepared to step in if and when a failure among issuers threatens consumer privacy. The Commission should actively monitor how issuers implement any use or disclosure of consumer data, regardless whether the data contains identifiers or not. We emphasize what we said in earlier comments. Consumer loan data will be readily identifiable even if all overt identifiers are removed. This is especially true for mortgage loans. So much consumer data and so much real estate information is available from private and public sources that re-identification of mortgage loans is simple and inexpensive to do. Other consumer loan data is also readily re-identifiable.

If the responsibility is to be given to a private entity like an issuer, then the terms and conditions of the basic operation need to be more detailed, and the obligations of issuers and data users need to be stated much more expressly.

B. Concern: The FCRA and its Relevance for Borrower Data

One particular concern we have is that the memo's reference to privacy laws fails to take note of the state of privacy legislation in the United States. The memo suggests that some borrower data could fall under the Fair Credit Reporting Act's controls, procedures, and protections at least

some of the time. This may be true, but only up to a point. The FCRA is not designed for the proposed type of databases or database owners contemplated here, and it will not be relevant much of the time because of the law's exceptions or limited reach. Further, much financial data about consumers has, through various methods, leaked into commerce outside of the FCRA's protections. The data is then used in ways that affect a consumer's financial, insurance, employment, and other marketplace opportunities, in some cases with substantial consequences.

The World Privacy Forum just (April 2014) released a report on predictive analytics and consumer scoring that documents in some detail some of these largely unregulated activities. The report is *The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future*, available at http://www.worldprivacyforum.org/category/report-the-scoring-of-america/. Here is a short summary of the report:

> This report highlights the unexpected problems that arise from new types of predictive consumer scoring, which this report terms consumer scoring. Largely unregulated either by the Fair Credit Reporting Act or the Equal Credit Opportunity Act, new consumer scores use thousands of pieces of information about consumers' pasts to predict how they will behave in the future. Issues of secrecy, fairness of underlying factors, use of consumer information such as race and ethnicity in predictive scores, accuracy, and the uptake in both use and ubiquity of these scores are key areas of focus.
>
> The report includes a roster of the types of consumer data used in predictive consumer scores today, as well as a roster of the consumer scores such as health risk scores, consumer prominence scores, identity and fraud scores, summarized credit statistics, among others. The report reviews the history of the credit score – which was secret for decades until legislation mandated consumer access — and urges close examination of new consumer scores for fairness and transparency in their factors, methods, and accessibility to consumers.

What the WPF consumer scoring report documents is that there is a vast appetite for consumer information, especially financial information that can be acquired outside of FCRA rules and protections. Many existing consumer scores make use of financial information or proxies for financial information. Even if data on individuals or households is not available, those who engage in consumer scoring use neighborhood data and apply that data to individuals, fairly or not. Thus, even aggregated statistical data can be used in ways that affect individual consumers and households. The point is that there is a constant and pressing demand for consumer financial data of all sorts, and those who engage in consuming scoring (let alone identity thieves) will seek to acquire any data that they can.

The financial information attached to mortgages, car loans, and other consumer borrowing activities is very attractive to the consumer data industry. Some of this information will reveal directly a most desired class of data, namely actual income data for individuals and households. The consumer data industry sometimes has approximate income data, limited salary data, and other proxies for income, but complete income data can be hard to obtain. **Asset-level data is**

highly desirable, and highly desirable data will attract consumer industry users as well as crooks.

C. Concern: Most Consumer Data is Not Protected by Privacy Laws

A second point is that much consumer data is not protected by any privacy law at all. The FCRA protects credit reports, but as the WFP consumer scoring report shows, financial data outside the FCRA's umbrella is used every day by marketers, data brokers, profilers and others. Marketing data is mostly unregulated for privacy. Many companies buy and sell consumer data for marketing purposes every day without limit or consumer rights. The Commission cannot assume that existing privacy laws will cover asset-level data or protect consumer privacy interests because legal protections in this area are largely irrelevant or inapplicable.

In this arena, privacy laws other than the FCRA offer no help to consumers. Gramm-Leach-Bliley provides consumers with highly limited privacy protections at banks. Banks can easily evade the consumer protections by choosing to share information with their "affiliates", and almost anyone can be a bank affiliate. The health privacy rules issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) apply only to health records maintained by health care providers, health plans, and health care clearinghouses. Health data disclosed by HIPAA covered entities is generally outside the HIPAA regulatory scheme. Health data acquired by websites, merchants, marketers, and others is wholly unregulated for privacy. *In fact, no privacy law at all applies to most consumer data in the hands of most private sector entities*. The Commission should not assume that issuers who provide consumer data to investors would be subject to any privacy law whatsoever. Asking for innovation in the application of privacy laws would be more acceptable if there were actually privacy laws that covered the data and the data processors.

If the Commission proceeds with the plan outlined in the Corporation Finance Memorandum, consumers need a host of additional protections to make sure that their data does not leak out of the controlled environment that the memo envisions. The Commission must find a way to provide the privacy protections that no existing law provides.

IV. Recommendations

We have several suggestions regarding the proposal, which we discuss below.

A. Chain of Custody

All asset-level consumer data (whether or not it has overt identifiers) should be subject to a chain of custody so that the data remains subject to a common core of privacy and security rules. If an issuer provides data to an investor, the investor should be subject to privacy and security rules. If an investor shares data with another investor, the second investor should be subject to the same privacy and security rules. A model here is the business associate provisions of HIPAA. A

hospital may share patient data with lawyers, accountants, and contractors, but HIPAA requires that the same privacy and security rules that apply to the hospital also apply to those who process patient data on behalf of the hospital. That same chain of protection is needed here.

B. Data Use Agreements and Fair Information Practices

The best method for establishing is a formal law or regulation, and we urge the Commission to establish specific privacy and security rules for asset-level data about consumers that reflect the requirements of Fair Information Practices (FIPs).[2] We would push that idea harder, but we see no evidence that the Commission is willing to consider that option. A regulation would provide a level playing field for issuers, and the same degree of privacy protection for consumers.

We observe that a Commission rule need not provide all the details that a privacy and security rule might otherwise have. The Commission could establish a short rule that requires use of a data use agreement for all asset-level data transfers and that provides high-level requirements for a data use agreement that each data user must sign.[3] The rule would allow for enforcement by the Commission and, perhaps, by others like the CFPB. A rule establishing a framework for data use agreements is a middle ground between a full-fledged privacy and security regulation and reliance on contract or tort law exclusively.

If the Commission does not establish a rule for data use agreements, data use agreement would still be the instrument of choice for governing asset-level data access. Every issuer should be required to have each user or recipient of data sign a data use agreement. The HIPAA equivalent in some ways is a business associate agreement, but HIPAA is different because business associate agreements apply only to those who process data on behalf of the HIPAA covered entity. Here, asset-level data users will be processing data for their own purposes. Nevertheless, a data use agreement offers the best way to inform users of their privacy and security obligations.

C. Transparency

Each issuer that holds asset-level data, whether for its own use or for sharing with potential investors, should have a privacy and security policy published on a public-facing website. Because issuers are the starting point for a chain of custody and data use agreement, it is important that they have clear, complete, and public policies. The baseline must be adequate or everything that follows will be built on sand.

---

[2] For more information on the history and current use of FIPs by the Obama Administration, see Robert Gellman, *Fair Information Practices: A Basic History*, http://bobgellman.com/rg-docs/rgFIPShistory.pdf.

[3] A proposal for a legislative framework for data use agreements by Robert Gellman in *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 Fordham Intellectual Property, Media & Entertainment Law Journal 33 (2010), might be useful here. The framework allows a data discloser and a data recipient to enter into a contract that defines responsibilities and establishes rules and enforceable standards under a statutory (or in this case, regulatory) scheme. That proposal covers deidentified data, but it would work in other contexts as well. http://bobgellman.com/rg-docs/RG-Fordham-ID-10.pdf.

D. Specific Elements of Data Use Agreements

A data use agreement as discussed above should include at least the following elements:

1. A rule strictly limiting use of the data by an authorized recipient to the specific investment purpose for which the data was made available and in accordance with the data use agreement. The data – and any data derived from the asset-level data – may not be used for any other activity or line of business that the recipient may undertake.

2. Qualification of recipients. Before disclosure of any asset-level data to a potential investor, the investor must meet qualification standards. The industry already knows how to qualify investors for classes of investment. Qualification is essential lest the data falls in the hands of a person who lacks the requisite intent or ability to sue the data for the intended purpose and to honor the limits on maintenance, use, and disclosure.

3. A flat prohibition on the disclosure of the data to anyone for an unrelated purpose, and a requirement that any disclosure for a related purpose be accomplished only through a data use agreement that has the same requirements (including limits on use and disclosure) that apply to any recipient. The requirement for a data use agreement would apply, for example, to a disclosure to the recipient's lawyer, computer service firm, or investment advisor.

4. A requirement that each recipient of asset-level data must have in place a privacy and security policy for the data that meets the standards of the data use agreement.

5. A requirement that any recipient of asset-level data must erase or otherwise destroy the data at the earliest opportunity consistent with the purpose of the disclosure. Not all consumer data transferred to an investor should be destroyed any later than six months after its acquisition by the investor.

6. A requirement for industry standard physical, administrative, and technical safeguards. The Commission need not reinvent the wheel here. Existing security requirements from GLB or HIPAA can be readily repurposed for asset-level data. All data, whether at rest or in motion, should be encrypted using a technology at least as robust as that required for patient data under HIPAA.[4]

7. A requirement that all who maintain asset-level data must have in place an adequate plan to address security breach. It is inevitable that there will be a security breach, and advance planning is important if a prompt response will occur. The data use agreement should include a ban on moving asset-level data to any jurisdiction that does not have an applicable security breach notification law. Each data use

[4] See http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

agreement should also specify whether and how the discloser and recipient will share responsibility for responding to a data breach.

8. The consumers who are the data subjects of any asset-level data should expressly be made third party beneficiaries of the data use agreement. This will enable consumers to sue over the misuse of their data. In addition or in the alternative, any holder of asset-level data that allows consumer data to be used for marketing, profiling, or in any other way prohibited by the data use agreement should be liable for liquidated damages of $1000 per individual in addition to any actual damages. It should not matter whether the misused data contains overt identifiers because it is easy for any knowledgeable person to add identifiers. A consumer should be entitled to liquidated damages upon a showing that that the misused data is about the consumer.

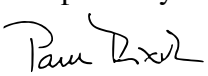
9. Anyone found to have added any asset-level data (whether it contained overt identifiers or otherwise) to any marketing list, consumer profile, or other database used for credit, insurance, employment, marketing, consumer scoring, profiling, or advertising purpose must immediately remove all data from the database. If removal is not possible, then the entire database must be entirely erased or destroyed. We are fully aware that if a data broker uses the asset-level data improperly and cannot fully remove all traces from its database, the database would lose all its entire economic value. This is intended to be the data equivalent of a death penalty for anyone misusing the data.

10. Any violations of a data use agreement must be immediately reported to the Commission for public posting. Anyone responsible for misuse of data should be barred from access to similar data for ten years.

Unless these measures become part of the access and use standards for asset-level data, the proposal of the Division of Corporation Finance will not include sufficient privacy protection for consumers, and the risk of data sharing will exceed the benefits. We remind the Commission, as we did before, that privacy and security protections for asset-level data is essential for many reasons. Our concern is for the privacy of consumers, and we are pleased that the Commission shares that concern. But another reason is that misuse of the data will threaten the stability of asset-backed instruments by placing all borrowers at greater risk to be victims of criminal activity and thereby lowering the value of the asset-backed instruments. In this respect, issuers and investors share interests with consumers. However, we doubt that the nexus between security and privacy will be clear to all issuers and investors, which is why we urge strong restrictions and sanctions.

We thank the Commission again for the opportunity to comment, and we stand ready to assist in the future in any way we can.

Respectfully submitted,



Pam Dixon