CrowdFund Intermediary Regulatory Advocates
1345 Avenue of the Americas
New York, NY 10105
Telephone: (212) 370-1300

February 4, 2014

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

RE: File No.: S7-09-13; Data Scraping, Fraud, and Privacy Concerns, Release: 33-9470

Dear Ms. Murphy:

I am writing you on behalf of the Crowdfund Intermediary Regulatory Advocates ("CFIRA"), a crowdfunding trade organization that lobbies and advocates for regulations that will support the crowdfunding industry in connection with Title II and Title III of the Jumpstart Our Business Startups Act of 2012. CFIRA's role is to protect the interests of investors and issuers, and advance the common business interest of intermediaries and third party service providers in the securities industry. Our members are comprised of intermediaries (broker-dealers and funding portals), issuers, investors, and third party service providers who are engaged in or who intend to engage in business under Titles II and III.

In reading through the intermediary requirements for displaying issuer information reflected in Commission Release Nos. 33-9470, 34-70741, File No. S7-09-13 (the "Rule Proposal"), at first glance it appears logical to mandate that all information about a particular transaction be made publicly available on the intermediary's platform. However, with further analysis we feel this notion of making everything public about a transaction, without requiring a person to register for a basic membership account with the intermediary's website, opens up the opportunity for increased fraud in the space. Less prominent, but also of a major concern, it also causes privacy concerns for small businesses. We completely understand this was not the intent of the Commission and the proposal is more about satisfying the requirements to make all information public to allow the Commission, FINRA and other interested parties, such as state regulators, to access information without impediment. Because of this, we are writing to address these issues and offer a simple solution that will solve these areas of concern.

The concept of Data Scraping

Before addressing the issue of data scraping and how we feel it will potentially undermine certain investor protections, we feel it's important to first define what it is. Data scraping (sometimes referred to as screen scraping or web scraping) is a technique in which a computer program (in this case) extracts data from human-readable output coming from a publicly accessible website. The program works behind the scenes to navigate a website, copy its contents, and store that information in another location outside of the original site. Not only can data of a website be scraped and copied, but visual elements as well.

A popular example is when a program is developed to crawl and scrape a website to copy the contents of

the site with a malicious strategy or intent in mind. Sometimes this activity is done to steal data or replicate a website for its own purposes. A very common instance is with YellowPages.com; the business directory data on their website is open and accessible to the public - it is very easy to scrape this data and create a business directory site or use the listings data for one's own purpose. It's specifically this example, of how data can easily be copied and replicated, which opens a great area of concern and we feel can lead to the potential of increased fraud.

Requirements under Section 4A(d)

Section 4A(d) requires the Commission to make, or cause the intermediary to make, offering statements and annual reports available to states. We understand this and feel that having the intermediary submit and file all information with EDGAR is enough to satisfy these requirements of making it fully open and public to the Commission, FINRA and other interested parties, such as state regulators. To impose additional obligation on the intermediaries to make all information about a transaction publicly available on their platform, without a membership account to view the information, does nothing more to satisfy the requirements under Section 4A(d) and makes intermediaries vulnerable to possible fraud.

Decreasing Investor Protection

We feel that is critically important that the Commission not mandate that all information regarding a deal is made publicly available on the intermediary's website, without a potential investor being a registered member of that intermediary. We agree with making certain information on the pitch page publicly available and visible to all users, regardless of membership level. This would include information such as company description, pitch video, executive team, type of securities being offering, terms of the deal, etc. But as it relates to disclosure documentation such as financial statements, use of proceeds, legal disclosures, certification of incorporation, etc., we believe that it is important to allow the intermediary to retain these documents behind a membership registration.

As with all membership-based websites, it is critically important that certain information be managed behind a registration wall. Forcing users to simply register for a basic account and verify their email address (by clicking a link in their email) to gain access to this information is very important to the entire industry and can greatly reduce the potential unintended consequences, fraud. We are not suggesting the user needs to "open a full account" with the intermediary, but merely a basic membership by entering their name and verifying their email address.

Having all information made publicly available on an intermediary's site, without a basic member account, will open up the ability for people to develop programs to run against the intermediary and scrape its data and documents. This information can then be copied over to an un-registered and non-approved funding portal where the potential for securities fraud can happen. Simply forcing users to verify that they are a physical person, and not a malicious program, can eliminate this from happening and give the intermediary greater control over the security of their website.

The question definitely arises whether this idea would apply equally to EDGAR since much of this information will be submitted to EDGAR and will already be made publicly available. We do not feel this is exactly the same since EDGAR has limitations on their data-handling and will not be setup to receive and display all types of data, documents, videos, PowerPoint presentation, etc., the way such documents or other information will be viewable on an intermediary's website. Scraping the EDGAR system may happen and probably does today but the limitation of data handling will work out in the industry's favor and will not allow the same level of scraping that may be performed on an intermediary site to copy their code and visual elements, copy all information as it appears in the format on an intermediary, and then creating a replica of that intermediary.

We highly recommend allowing the intermediaries to provide a multi-tiered member registration process on their platform and not mandating that everything be made public. A multi-tiered registration process would provide two levels of access: Member and Investor. A Member would have access to all information once they have completed a simple registration process. The Investor would be the same as a Member but has provided the necessary information and credentials required to "open an account" with an intermediary and be ready to make an investment in an offering.

This is the right of the intermediary; security and back-end data management should be of the responsibility of the intermediary.

Recommendations:

1) Allow the intermediaries to hide the most important financial and legal disclosures of an issuer behind a simple member registration process. The recommended steps for the intermediary registration process flow would include two possible methods:
    a. Manual Registration
        i. Complete fields in registration form on intermediary
            1. First name
            2. Last name
            3. Email address;
        ii. Intermediary automatically sends user an email with a link to verify their email address, which they just entered;
        iii. User checks their email account for an email from the intermediary and clicks the link in the email, confirming they have access to that email address; and
        iv. The user's account is now verified and all issuer documents and disclosure can be accessible on the intermediary's platform, across all available actively-funded deals.
    b. 3rd Party Authentication – (e.g., oAuth)
        i. oAuth is an open standard for authorization used by many large 3rd Party Social Media platforms such as Facebook, LinkedIn, Google+, Twitter, etc.; and
        ii. oAuth is used to authenticate an individual's identity on one of these 3rd Party Social Media Platforms, the concept would be the same as the manual registration and provide even more details on the individual.
2) Now that the user's email address is verified or authenticated via a 3rd Party Platform, it will allow for further due diligence on the intermediary:
    a. The intermediary can now see who has registered on their platform
    b. The intermediary can now monitor and track all users for malicious activity
    c. In the case where malicious activity is happening, the intermediary can pause, deactivate, or delete any account where malicious activity is being performed
    d. In the case where malicious activity is happening, the intermediary now knows the IP address of the user and can block that IP from using their platform

Thank you for your consideration on these suggestions. We are open to ongoing discussions to help address the Commission concern on this and how to work together to help protect this industry.

Sincerely,

Daryl H. Bryant
Founder and CEO, StartupValley
Board Member, CFIRA
Co-Chair, Portal Committee

Chris Tyrrell
Founder and CEO, OfferBoard
Chairman, CFIRA

CROWDFUND INTERMEDIARY REGULATORY ADVOCATES