May 9, 2022

U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure File Number S7-09-22

Thank you for the opportunity to provide comments to the proposed rules.

My name is Rocio Baeza. I am a working professional, wife, mom to 2, and a data privacy advocate. I am the CEO and Founder of CyberSecurityBase, a Chicago-based consultancy that specializes in the small-dollar lending space, helping Legal and Compliance Executives with information security and compliance initiatives.

Our professional services include serving as our clients' outsourced security and compliance team, developing and implementing a customized set of information security[1] policies and procedures, performing audits, conducting gap assessment, and/or providing SOC2 readiness support.

After graduating with a B.A. in Mathematics from the University of Chicago, I started my professional career at CashNetUSA. CashNetUSA was a rising payday lender that grew into what is now known as Enova International, a publicly traded company with an international presence in the financial services and data analytics space. While employed at Enova, I supported recognizable brands, including Cash America, NetCredit, QuickQuid, Pounds to Pocket, and Enova Decisions.

My professional background provides me with a unique perspective that I seek to share, to educate regulators, influence regulation and guidance from agencies that regulate the financial services industry. The end goal is to ensure that regulations protect the everyday American consumer from negative impact resulting from inadequate protection of personal information processed by the financial services industry. This is congruent with the SEC's mission to protect Main Street investors and others that rely on the markets to secure their financial future.

Since my time at Enova, I have supported clients on a consultant basis, spoken at professional trade events, and voiced concerns with the current state of the cybersecurity field to regulators.

At the local level, this includes assessing data security measures for the Chicago CityKey ID (a government-issued ID card for Chicagoans).

[1] Note that the terms information security, security, and cybersecurity are used interchangeably and have the same meaning: the protection of data that is available in a digital format

At the federal level, this includes providing commentary to the proposed changes to the GLBA's Safeguards Rule, participating in the FTC's Safeguards Rule Virtual Workshop in July 2020.

In 2021, I submitted commentary to additional areas, including the CFPB's Section 1033 - Consumer Access to Financial Records Proposed Rule and Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, including Machine Learning,

My work experience includes roles in various key roles, including data analytics, product management, IT risk management, cybersecurity, and compliance. Combined with my early journey as a CEO, I have a unique perspective that can provide insights that will help the SEC in finalizing the proposed rules.

As it relates to enhanced and standardized disclosure on the registrants' cybersecurity risk management, strategy, and governance, the proposed amendments are too subjective. If implemented as described, my concern is that they will create a significant reporting burden to registrants and provide no meaningful information for an investor that wants to understand a registrant's cybersecurity risk management capabilities.

In the following paragraphs, I will illustrate what I mean and then follow with recommendations for a more effective approach.

The SEC is considering amending Form 10-K to require disclosure of a registrant's policies and procedures, for identifying and managing cybersecurity risks.

As worded, the proposed amendment implies that a registrant is able to identify and manage cybersecurity risks with the mere existence of policy and procedures. This is incorrect. An organization ***needs*** to establish a number of foundational elements ***before*** it can assess cybersecurity risks. We stress the importance of these foundational elements, when developing and implementing cybersecurity programs with our clients. These include:

- **data inventory:** this clarifies the data held by the organization
- **data flow diagram:** this illustrates how the organization receives data and where it flows after it in its possession
- **IT asset inventory:** this tracks where the organization processes and/or stores data
- **3rd party vendor inventory:** this tracks the parties that exchange data with the organization
- **data security and privacy requirements inventory:** this tracks laws, regulations, standards, and/or frameworks that the organization is required to follow (or has made commitments to follow)
- **cybersecurity vision:** this clarifies the results that the organization desires from its cybersecurity program

- **cybersecurity risk tolerance:** this defines what is acceptable and what is not

Only ***after*** this information has been gathered, can an organization ***start*** the process of assessing cybersecurity risks.

I urge the SEC to consider amending Form 10-K to require that the registrant disclose the following information ***with*** the following structure.

Disclosure Item	Response
Data Inventory	
Does the registrant have a data inventory? *The data inventory is a record of the data held by the registrant and serves as the authoritative data inventory.*	_Yes _ No
Has the data inventory been reviewed within the last 90 days?	_Yes _ No
Will the data inventory be reviewed and updated in the next 90 days?	_Yes _ No
Data Flow Diagram	
Does the registrant have a documented data flow diagram? *The data flow diagram is a visual illustration that demonstrates how the registrant receives data and where it flows once it is in its possession. This data flow diagram must serve as the authoritative data inventory*	_Yes _ No
Has the documented data flow diagram been reviewed within the last 90 days?	_Yes _ No
Will the documented data flow diagram be reviewed and updated in the next 90 days?	_Yes _ No
IT Asset Inventory	
Does the registrant have a documented IT asset inventory? *The IT asset inventory is an inventory of all systems and/or services (in-house or external) that processes and/or stores data in its possession. This IT asset inventory must serve as the authoritative data inventory*	_Yes _ No
Has the documented IT asset inventory been reviewed within the last 90 days?	_Yes _ No
Will the documented IT asset inventory be reviewed and updated in the next 90 days?	_Yes _ No

3rd Party Vendor Inventory	
Does the registrant have a documented 3rd party vendor inventory? *The 3rd party inventory is a record of all external parties that provides a service to the registrant and indicates the type of data that is exchanged. This 3rd party vendor inventory must serve as the authoritative data inventory*	_Yes _ No
Has the documented 3rd party vendor inventory been reviewed within the last 90 days?	_Yes _ No
Will the documented 3rd party vendor inventory be reviewed and updated in the next 90 days?	_Yes _ No
Data Security and Privacy Requirements Inventory	
Does the registrant have a data security and privacy requirements inventory? *The data security and privacy requirements inventory is a record of all laws, regulations, standards, and/or frameworks that the registrant is required to follow (or has made commitments to follow)*	_Yes _ No
Has the data security and privacy requirements inventory been reviewed within the last 6 months?	_Yes _ No
Will the data security and privacy requirements inventory be reviewed and updated in the next 90 days?	_Yes _ No
Cybersecurity Vision	
Does the registrant have a documented cybersecurity vision that has been presented to the Board of Directors? *The cybersecurity vision describes the results that the registrant desires from its cybersecurity program. It must have been presented to the Board of Directors*	_Yes _ No
Has the cybersecurity vision been reviewed within the last 12-month period?	_Yes _ No
Will the cybersecurity vision be reviewed and updated within the next 12-months?	_Yes _ No
Cybersecurity Risk Tolerance	
Does the registrant have a documented cybersecurity risk tolerance that has been presented to the Board of Directors? *The cybersecurity risk tolerance defines thresholds for behavior, activity, or events that are acceptable (and those that are not)*	_Yes _ No

Has the documented cybersecurity risk tolerance been reviewed within the last 12-month period?	_Yes _ No
Will the documented cybersecurity risk tolerance be reviewed and updated within the next 12-months?	_Yes _ No

Requiring these disclosures in this format, accomplishes the following:

- It educates registrants of the foundational elements that an effective cybersecurity risk management program requires; *These foundational elements are the equivalent of bookkeeping in the field of Accounting*
- It removes the subjectivity of the disclosure, and provides clear information to the investor; *The existence of a policy or procedure is not useful information for an investor; An investor benefits in knowing if the registrant has a good understanding of the data held, the location of data processing and storage systems, the flows of data, and digital boundaries of the registrants*
- It communicates the Board's familiarity with the registrant's cybersecurity vision and risk tolerance; *The investor benefits in knowing if the registrant has articulated regulatory and stakeholder requirements, vision, and risk tolerance levels and communicated all this information to the Board of Directors*
- Most important, it democratizes the concepts needed by organizations that do not have a Chief Information Security Officer; *This clarifies the foundational elements that a non-experienced security owner needs to be aware of, to help its organization identify and manage cybersecurity risks*

Having supported online lenders with 3rd party due diligence programs (also known as vendor management programs), and being on both sides of the diligence conversation, I am confident that this reporting format and structure will meet the goals of the proposed rules[2]. In my experience, asking contextual and specific questions are a more effective way of gathering meaningful information. As proposed, the administrative cost to meet the proposed requirements are greater than the value of the information made available by the proposed disclosures.

The SEC is considering amending Form 10-K to require disclosing whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation.

As worded, the proposed disclosure may encourage registrants to find creative ways to answer "yes" to this question. A serious executive would never dare to imply that they are running an organization that does not include cybersecurity considerations. Our team has personally

[2] Better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of material cybersecurity incidents.

witnessed this, in advising our clients in cybersecurity and compliance topics during the due diligence phase of a partnership with a US bank.

I urge the SEC to consider amending Form 10-K to require that the registrant disclose this information in the following structure and format:

Cybersecurity Considerations in Business Strategy	
Does the registrant have a documented cybersecurity vision that takes into account:	
the interests of the Board of Directors?	_Yes _ No
the interests of investors?	_Yes _ No
the interests of its customer base?	_Yes _ No
Cybersecurity Considerations in Financial Planning	
In reviewing the spend for the past 12-months, did the registrant allocate at least 3% of its annual spend to support cybersecurity risk management? *(A note for the SEC: The percentage is arbitrary. It is meant to provide some objectivity to the question.)*	_Yes _ No
Has the registrant allocated at least 3% of its budget, for the current budget period? *(A note for the SEC: The percentage is arbitrary. It is meant to provide some objectivity to the question.)*	_Yes _ No

Requiring these disclosures in this format, accomplishes the following:

- it removes the subjectivity of the disclosure, and provides clear information for the investor; this clarifies if the registrant's cybersecurity vision takes into account the interests of all key stakeholders or only some; *The affirmative confirmation to cybersecurity considerations to strategy, financial planning, and capital allocation is not useful information for an investor; An investor benefits in knowing specifics about these areas*
- it communicates the resources that the registrant has made available for managing cybersecurity risks in the last 12-month period and the current budget period

The SEC is considering amending Form 10-K to require disclosure specified in proposed Item 106 regarding:

- **A registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks**

As worded, it is suggested that the proposed disclosure will be an open ended question. Assuming that this is true, this creates a low bar for the registrant to report that the Board is involved at a greater capacity than it actually is.

I urge the SEC to consider amending Form 10-K to require that the registrant disclose this information in the following structure and format:

Board Oversight Regarding CyberSecurity Risks	
Has the registrant presented the Board of Directors with results of a security risk assessment performed in the last 12 months?	_Yes _ No
Has the registrant presented the Board of Directors with remediation plans and progress updates for the top 3 cybersecurity risks?	_Yes _ No
Has the registrant updated the security risk register to capture the remediation plans and progress updates for the top 3 cybersecurity risks?	_Yes _ No
Has the registrant made the security risk register available in its entirety to the Board of Directors for awareness and review?	_Yes _ No

Requiring these disclosures in this format, accomplishes the following:

- it provides registrants with a roadmap for communicating cybersecurity risks to the Board; *Historically, cybersecurity reporting has been challenging, because of the translation that the security owner needs to do when discussing cybersecurity with business-minded executives*
- it provides investors with clarity on specific actions that have been carried out to keep the Board informed on cybersecurity risks

The SEC is considering amending Form 10-K to require disclosure specified in proposed Item 106 regarding:

- **Management's role, and relevant expertise, in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.**

As worded, it is suggested that the proposed disclosure will be an open ended question. Assuming that this is true, this creates a low bar for the registrant to report that Management plays an active role and has relevant expertise in managing cybersecurity risks as described.

I urge the SEC to consider amending Form 10-K to require that the registrant disclose this information in the following structure and format:

Management Role and Experience in Managing CyberSecurity Risks

Has the registrant performed a security risk assessment within the last 12-months and that is documented?	_Yes _ No
Does the security risk assessment capture the criteria used for the evaluation and categorization of identified security risk or threats faced by the registrant?[3]:	_Yes _ No
In the last 12 months, has the registrant assessed at least 80%[4] of its IT assets, to measure compliance to the documented security policy requirements? *In other words, has management set the expectation that the documented security policy requirements are to be applied to all IT assets? Or only specific IT assets?*	_Yes _ No
In the last 12 months, has the registrant communicated to the Board the percentage of IT assets that have been assessed for compliance to the documented security policy requirements?	_Yes _ No
Currently, does the registrant have a set of documented procedures that align to the documented security policy requirements and reflect current practices being performed by the registrant?	_Yes _ No
In the last 12 months, has the registrant communicated to the Board the percentage of security policy requirements that are not supported by documented procedures (or do not align to current practices being performed by the registrant)?	_Yes _ No
Does the registrant affirm that the security policy and procedures align to the letter and substance of the published Privacy Policy (or Privacy Notice)?	_Yes _ No

Requiring these disclosures in this format, accomplishes the following:

- it introduces standardization and rigor to the security risk assessment process; *This is important, as the cybersecurity industry has not yet matured to have an established standard for assessing security risk; this creates a disadvantage for the registrant that relies on external support and may not have the skillset to determine if a service provider is providing a quality security risk assessment*
- it provides Management and the Board with visibility on the efforts around implementing and operationalizing security policy at the IT system level; *Historically, the cybersecurity industry has failed in providing meaningful reporting to C-level executives and the Board. This can be remedied by guiding Management on the importance of delivering customized security reporting that is contextualized to the IT systems that support the business*

[3] Note that this aligns to the 2021 update to GLBA's Safeguards Rule (314.3 Standards for safeguarding customer information)

[4] 80% is an arbitrary figure; The goal here is that this metric be quantifiable;

- it provides Management and the Board with visibility on the compliance levels for its IT systems; *Historically, the cybersecurity industry has failed in providing meaningful reporting to C-level executives and the Board. This can be remedied by guiding Management on the importance of delivering customized security reporting that is contextualized to the IT systems that support the business*
- it clarifies to Management that a documented policy is not sufficient to manage cybersecurity risks; *When regulations start by requiring security policy, it tends to shift the focus away from "meaningful activity" to "administrative activity" that comes off as robust, but ineffective, because of the lack of focus placed on operationalizing supporting procedures across the data processing environment level*
- it sets the expectation that the Privacy Policy (also known as a Privacy Notice) that is public-facing, needs to align to the information security policy, which is directed to internal teams; *This is a gap that has been created because of the misalignment between legal and security industries, that can start to be remedied with the proposed rules*

In closing, I appreciate the invitation to provide comments on the proposed Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. This is an important matter, as it impacts institutional and everyday investors.

Please consider this information and these recommendations as you finalize the rules.

I invite you to reach out if you would like to discuss these comments and recommendations further.

Sincerely,
Rocio Baeza
CEO and Founder
CyberSecurityBase
[redacted]