October 18, 2021

Thank you for inviting the public to comment on the Proposed Interagency Guidance on Third-Party Relationships: Risk Management.

This response is structured to provide information on my professional work experience, provide actionable recommendations for specific areas highlighted for public commentary, and in some cases, provide sample templates to illustrate specific recommendations.

My name is Rocio Baeza. I am based in Chicago, a working professional, mom of 2, spouse, and data privacy advocate. I am the CEO and Founder of CyberSecurityBase, a consultancy that helps Legal and Compliance Executives with information security and compliance initiatives. The team specializes in the online small-dollar lending space. This may be in the form of an outsourced security and compliance team or customized development and implementation support of policy and procedures that address laws and regulations focused on protections in consumer lending. 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.

Since then, 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). 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, and in 2020, joined as members of the the Online Lenders Alliance to engage with industry leaders and regulators in conversations of information security and compliance to federal consumer protection laws. 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 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.

I thank you in advance for your time in reading my remarks and consideration, as the agencies finalize the guidance. Please note that a supplementary video on this matter is available at: https://cybersecuritybase.com/thirdpartyrisk

A. Recommendation: Develop and publish educational resources that further guides a bank in developing a <u>customized</u> 3rd party risk management program that <u>standardizes the information being seeked</u> in the information gathering process and <u>standardizes Board/management reporting for oversight</u>.

This recommendation addresses the following specific requests for comment:

- *#6: How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?*
- *#9: What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?*
- *#13: In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?*
- *#14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?*
- *OCC's 2020 FAWs on Third Party Relationships: More specifically, the agencies seek public comment on whether: (1) any of those concepts should be incorporated into the final guidance; and (2) there are additional concepts that would be helpful to include.*

The financial services industry has been required to build 3rd party risk management programs, oftentimes, without in-house risk management expertise, resulting in developing programs that are highly resource intensive but oftentimes ineffective. The result is an industry that is engaging in due diligence exercises that are resource intensive for both parties, extends timelines for a decision, leaves 3rd party partnership decisions made with incomplete (or irrelevant) information, and a situation where the soundness of the banking industry and consumer protections are at stake.

Risk management is an area that requires years of experience and a targeted set of skills. This applies to 3rd party risk management. As regulations have evolved, the banking industry has been required to implement risk management programs and then mature the rigor of such programs. Risk management is a process that needs to be carried out in a systematic manner. However, it requires that foundational elements be established, for a party to be able to identify, analyze, and make a decision on a risk.

A banking organization cannot effectively manage 3rd party risk without establishing foundation elements. These include establishing the organizational risk tolerance and identifying critical business functions. These elements are what should guide the structure of the 3rd party risk management program. In the 13 years of working in the

financial services/fintech/small-dollar lending/technology/compliance areas, in supporting 3rd party due diligence requests from a bank (or at the direction of a bank), it is concerning that 3rd party risk management programs are being built without these foundational elements. This is evident in the volume of questions being asked, in the types of questions being asked, in the policy document requests, and the training record requests. Unfortunately, it is common for a 3rd party to undergo the same due diligence process, where instead, they should have undergone a due diligence process that is tailored, based on the banking organization's risk tolerance levels and interconnectedness to a critical business function.

It is imperative that all banking organizations be equipped with knowledge and resources to develop and operationalize an effective 3rd party risk management program. There has been an emergence of tools and professional services that promise to help organizations manage third party risk, including my company CyberSecurityBase. However, when a banking organization (or any other type of organization) stands up a 3rd party risk management program that is not customized to their organization, that is not contextual to the risk tolerance and interdependency of a critical business function, it leads to a resource-intensive exercise that does not provide value to the banking organization, banking industry, organizations wanting to partner with banks, or everyday American consumers.

I urge agencies to form a working group to develop and publish educational resources that further guides a bank in developing a customized 3rd party risk management program, that standardizes the information being seeked in the information gathering process, and standardizes the Board/management reporting for effective oversight. Ideally, this working group would include regulators, executives of banks, attorneys in the consumer lending space, compliance professionals in the financial services space, and consumer advocates.

By providing educational resources on how to develop a customized 3rd party risk management program, the banking organization can trust that internal resources are being used effectively.

By providing sample templates that standardizes the information being seeked in the due diligence phase, it allows banks and banking organizations to develop a due diligence package that can be created once and shared with many parties, streamlining the process.

By providing sample templates that standardizes the Board/management reporting, the banking organization can trust that proper oversight is being provided.

By developing and publishing these educational resources, banking organizations and other providers partnering with banks will have access to resources that they can use to diligence and monitor their 3rd parties (i.e. a bank's 4th parties). This is an important step that will strengthen the American banking system, streamline the bank partnership due diligence and implementation cycle, introduce needed innovation in the financial services industry, and provide consumers with improved access to credit and financial services.

The CyberSecurityBase team is at your disposal to participate in this working group and openly share proven techniques that our consultants use with our clients. We are motivated to help because

- we support the spirit of the Proposed Interagency Guidance on Third Party Relationships: Risk Management
- we understand the value of education and simplification in the highly-regulated financial services industry
- we support responsible innovation in the banking sector, where the interests of both banks and consumers are being served

Below is a sample of what the educational resources can look like.

Practical Guide for Developing a Customized Third-Party Risk Management Program for a Bank

Step 1: Discuss with the Board and Management team to establish the bank's risk tolerance and third-party risk tolerance

Area	Guidance For Internal Use	Response
Organizational Risk Tolerance	*Describe the types of events or incidents that would be unacceptable to the Board and Management team. This can include risks related to service availability, legal and regulatory matters, customer experience, financial, reputational, and or social*	
Organizational Third-Party Risk Tolerance	*Describe the types of relationships or criteria that a third-party will need to meet, to be considered a good initial fit with the bank.*	

Step 2: Review the most recent Business Impact Analysis and capture the critical business functions in the inventory below

Sample Critical Business Function	Sample IT Systems	Recovery Priority
Receiving new loan/line of credit applications	• Workstation • Loan management system	1
Processing loan/line of credit applications	• Workstation • Headset • Reporting dashboard • Loan management system • CRA portal • IVR phone system	2
Funding approved applications	• Workstation • MFA Token • Loan management system • Docusign	3

	• Bank transfer portal	

Step 3: Establish the baseline factors that are to be considered when the bank is considering a third-party relationship

Modify the table below, to identify the areas that are most important for the bank. Once finalized, on the available column, articulate the threshold that the 3rd party must meet, for the Board and Management team to feel comfortable in proceeding with discussions on a partnership.

Area	Comfort Thresholds - Internal
Legal and Regulatory Compliance	
Financial Condition	
Business Experience	
Fee Structure and Incentives	
Qualifications and Backgrounds of Company Principals	
Risk Management	
Information Security	
Management of Information Systems	
Operational Resilience	
Incident Reporting and Management Programs	
Physical Security	
Human Resource Management	
Reliance on Subcontractors	

Insurance Coverage	
Conflicting Contractual Arrangements with Other Parties	
Contract Negotiation	
Nature and Scope of Arrangement	
Performance Measures or Benchmarks	
Responsibilities for Providing, Receiving, and Retaining Information	
Right to Audit and Require Remediation	
Responsibility for Compliance with Applicable Laws and Regulations	
Cost and Compensation	
Ownership and License	
Confidentiality and Integrity	
Operational Resilience and Business Continuity	
Indemnification	
Insurance	
Dispute Resolution	
Limits on Liability	
Default and Termination	
Customer Complaints	

Subcontracting	
Foreign-Based Third Parties	
Regulatory Supervision	

Step 4: Develop an external-facing version of the comfort thresholds, to share with potential third-parties during early conversations of a partnership discussion. Before distributing, ensure that an NDA is in place

Area	Sample Comfort Thresholds - External
Legal and Regulatory Compliance	Company has an in-house General Counsel that stays on top of regulatory developments and Head of Compliance that manages the CMS program
Financial Condition	Company has reached profitability
Business Experience	Company has been operating for 5 years or longer
Etc.	

Step 5: Formulate an *initial* 3rd Party Risk Management Due Diligence Questionnaire, based on the factors identified as critical for the bank to continue partnership discussions.

Consider documenting the questions below and once finalized, migrating to the tool of choice for capturing responses from 3rd parties participating in the due diligence process (i.e. Excel worksheet, cloud-based tool, GRC tool, etc)

Question	Response
1. How long has your organization been in business?	
2. Has your organization reached a level of profitability?	

3. Does your organization have in-house or outside General Counsel?	
4. Outside of General Counsel, does your organization have additional personnel supporting Legal and Compliance? If so, please describe.	
5. How does Legal stay on top of regulatory developments?	
6. Who manages the organization's CMS program?	
Etc.	

Step 6: Review the 3rd Party Inventory to ensure it is complete and has enough information to develop vendor types/categories that are tailored to the Bank

Vendor	Description	Categories
Loan Management System Provider	Primary LMS housing customer and loan account information	GLBA, US
Lead Provider USA	Lead aggregator	GLBA, Lead Provider, US, UDAAP
Lead Provider National	Lead aggregator	GLBA, Lead Provider, US, UDAAP
CRA Vendor 123	Credit reporting agency	GLBA, Lead Provider, US, FACTA, FCRA
CRA Vendor ABC	Credit reporting agency	GLBA, Lead Provider, US, FACTA, FCRA
Alternative Data Provider	Data reporting provider	GLBA, Lead Provider, US, FACTA, FCRA
Collections Agency USA	Outsourced collections team	GLBA, Debt Collector, US, FDCPA

Debt Buyer ABC	Debt buyer partner	GLBA, Debt Buyer, US, FDCPA
Google	Company-wide email, calendar, and document repository	Backoffice, GLBA
JIRA	Project management documentation and internal ticketing system	Backoffice
AWS	IT infrastructure provider	GLBA, US, Backoffice

Step 7: Identify core vendor types and develop due diligence questions that correspond to the critical areas, based on the vendor type.

Step 8: Review standard agreement templates to calibrate global vendor requirements and identify requirements for the identified core vendor types.

This helps ensure that expectations are captured at the contract level and that there is a safetynet to ensure congruence between due diligence responses and contract negotiations. It is recommended that any regular reporting requirements be included, along with sample reporting requests/templates.

Step 9: Standardize Board/management reporting

Sample 3rd Party Vendor Management Overview for the Board	
Total Volume	The bank is currently partnered with 25 3rd party vendors
Vendor Breakdown	12% Lending partners (3) 40% Technology providers (10) 12% Credit Reporting Agencies (3) 20% Alternative Data Providers (5) 4% Collection Agencies (1) 12% Debt Buyers (3)
Critical Vendors Volume	The bank has identified 9 critical 3rd party vendors
Critical Vendor Breakdown	33% Lending partners (3) 33% Technology providers (3) 33% Credit Reporting Agencies (3)
Rate of Vendors with Initial Due Diligence on File	80%
Rate of Critical Vendors with Initial Due Diligence on File	100%
Average Turnaround to Complete Initial Due Diligence	3 business days/vendor
Average Turnaround for Initial Feedback for a Contract Review	7 business days
Rate of Vendors with Annual Monitoring Diligence on File	30%
Rate of Critical Vendors with Annual Monitoring Diligence on File	100%
Average Amount of Time Needed to Complete Annual Monitoring Due Diligence	5 business days/vendor
Average Turnaround for Contract Renewal Review	3 business days
Most Common Request from Business	Expedited due diligence for key opportunities

Practical Guide for Developing a Third-Party Due Diligence Packet in Preparing for Discussions with a US Bank

Step #1: Assemble an inventory of applicable laws/regs and impacted areas for product(s) currently active

This is an inventory of federal laws and regulations that currently apply to the organization. This demonstrates that the organization has resources dedicated to identifying the laws and regulations that impact the consumer-facing products and analyzing how they impact the product.

Sample Organization	**Online Lender ABC**	
Current Service Offering	US-based online lender, providing personal loans and lines of credit for the sub-prime consumer lending market	
Regulation	**Applicability**	**Sample Areas of Impact**
ECOA *Equal Credit Opportunity Act*	Yes	• Eligibility criteria • Loan offer • Underwriting logic
UDAAP Unfair Deceptive Abusive Acts and Practices	Yes	• Marketing and advertising • Eligibility criteria • Loan offer • Loan servicing, including Collections • Complaints
MLA Military Lending Act	Yes	• No impact, as the APR and fee structure is under the 36% interest rate cap
FDCPA Fair Debt Collection Practices	Yes	• Collection campaigns

Step #2: Identify anticipated changes to applicable laws/regs and impacted areas post-bank partnership

This is an inventory of federal laws and regulations that the organization anticipates will apply, following a bank partnership. This demonstrates that the organization has compliance expertise to adequately assess regulatory impact for consumer-facing products that are being explored for the bank partnership.

Sample Organization	**Online Lender ABC**	
Anticipated Service Offering	LMS and underwriting services for banks to originate personal loans to the US sub-prime consumer lending market	
Regulation	**Applicability**	**Areas of Impact**
ECOA *Equal Credit Opportunity Act*	Yes	• Eligibility criteria • Loan offer • Underwriting logic
UDAAP Unfair Deceptive Abusive Acts and Practices	Yes	• Marketing and advertising • Eligibility criteria • Loan offer • Loan servicing, including Collections • Complaints
MLA Military Lending Act	Yes	• No impact, as the APR and fee structure is under the 36% interest rate cap
FDCPA Fair Debt Collection Practices	No	• The Bank will service loans in Collections

Red: Anticipated changes

Step #3: Prepare an initial due diligence packet

This is a standardized form that helps organize high level information about the status of the company and governance maturity. The idea is to capture information that will allow the bank executive team to determine if they feel comfortable moving forward with bank partnership discussions. This initial due diligence packet can be prepared once and used with multiple banks and banking organizations. This allows both banks and organizations to only invest in additional due diligence efforts for opportunities with a good organizational fit.

Due Diligence Area	Response
Provide a statement on Online Lender ABC's financial condition	
Provide bios of members of the Executive team, including qualifications and background	
Does Online Lender ABC have documented policies in place?	
Does Online Lender ABC have documented procedures in place?	
Does Online Lender ABC have a training program in place to ensure that personnel understand documented policy and procedures?	
Has it been communicated that Online Lender ABC personnel are expected to comply with company policies and procedures?	
To what extent does documented procedures align to current practices by Online Lender ABC personnel?	
Has Online Lender ABC managed a Compliance Management System for all existing products in the last 6 months?	
Will Online Lender ABC need	

access to bank data/systems?	

Step #4: Prepare a more targeted due diligence packet

This is a standardized form that helps organize additional detail that is relevant, given the products and services currently offered by the organization. The idea is to capture information that will allow the bank compliance executive further assess the organizational maturity and identify areas that would need to mature, for a formal bank partnership.

A sample is not being provided given the need to collaborate with industry professionals to develop a comprehensive list of organizational types and due diligence detail, from the perspective of a bank.

B. Recommendation: Update the guidance to require that banking organizations confirm with third parties that they create and maintain a data inventory, data flow diagrams, IT systems inventory, and 3rd party vendor inventory. These inventories are critical, as they are foundational for an effective information security risk management program.

This recommendation addresses the following specific requests for comment:

- *#17: What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*

  Information security and managing information security risks are complex areas, in part, because of the electronic nature of transactions, growing volume of information that is being captured, and the digital nature that the information is stored, shared, and processed. When banks and banking organizations first started to operate, this was handled over paper. Given the tangible form of information, it was clear when information was captured, where it was stored, and physical security measures to protect the tangible assets. At this time, information assets were represented in the form of paper documents, controlled by banking staff, organized in folders and filing cabinets, and located behind counters, in a building that had a security guard at the entrance and monitored for physical intrusions. Currently, we have a completely different environment that banks and banking organizations need to protect. Probably the most challenging part is not being able to "see" all the information that is being collected, stored, processed, and shared with other organizations.

  An information security program can only be effective when the bank or banking organization has established clear boundaries on the data it holds, the source of that data, how it travels within the organization, where the data is stored, and is clear about all parties that it shares data with.

  Below is a brief description for each of these foundational elements:

- **Data Inventory**: An inventory of data held by the 3rd party, the data source, the primary data system where the data sits, and the business need and use for the data point.
- **Data Flow Diagram(s)**: A visual illustration demonstrating how data is captured by the 3rd party, where it sits internally, the various paths that it may flow within the organization, and disclosures of data with both affiliates and non-affiliates.
- **IT Systems Inventory:** An inventory of all IT systems supporting the 3rd party. This should include all systems that an employee may need access to, to perform their job

responsibilities. Furthermore, it should include all systems, including in-house applications and 3rd party applications

- **3rd Party Vendor Inventory:** An inventory of 3rd party vendors and systems supporting the 3rd party (i.e. the banking organization's "4rd parties"). This should include the name of the vendor, a description of the services being provided, the type of data that they are authorized to process, and categorization as affiliate or non-affiliate partner.

In the 13 years of supporting financial service and providers in the small-dollar lending space, developing information security programs and compliance management systems, it is clear to me that organizations commonly lack in-house information security expertise. Given the rapid growth in the FinTech sector, evolution of technology, and mass aggregation of consumer behavior and personal data, without effective regulatory clarification, this creates risks for the everyday American consumer and jeopardizes the soundness of America's financial system. Currently, organizations without in-house information security expertise or access to outside resources are creating a situation where the organization is trying to figure this out on their own (and making little traction) or making investments that are not strategically aligned with business and compliance goals (and misses the mark that the regulation intended to meet).

By including capture and maintenance of these inventories, these guidelines will set clear expectations on the foundational elements that need to be put in place, for the 3rd party to be able to establish, operationalize, and maintain an effective information security program. This in turn, will set a critical new bar in the financial services sector, banking organizations, and strengthen information security posture for America's banking system as a whole.

C. **Recommendation: Update the to clarify that a banking organization's assessment of a third party's information security and risks needs to be tailored, such that the breadth and depth of the information security due diligence is appropriate, based on the data (or system connections) that is planned to be shared (implemented) with the third-party.**

This recommendation addresses the following specific requests for comment:

- *#17: What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*

In the 13 years of supporting financial service and providers in the small-dollar lending space, developing information security programs, and participating on both sides of the security due diligence process, it is demoralizing to see that the financial services industry commonly engages in third party due diligence activity, with little regard to the anticipated nature of the relationship. This leads to organizations using the same "ruler" when assessing third parties. This has created an administrative burden that oftentimes provides little value, requires that both parties invest in significant resources to support the activity, and in many cases, result in a "paper exercise" that misses the intent that regulation intended to meet.

D. **Recommendation: Update the guidance to highlight that when banking organizations are assessing the third-party's information security risk management program and risks, it needs to include any risks created for both the 3rd party vendor relationship and the customer.**

This recommendation addresses the following specific requests for comment:

- *#17: What additional information should the proposed guidance provide regarding a banking organization's assessment of a third party's information security and regarding information security risks involved with engaging a third party?*

The agencies are tasked with a specific set of responsibilities to the stability of the nation's financial system, effective operation of the US economy, soundness of the banking system, and in my opinion, the most important consideration, consumer protections.

In closing, I appreciate the invitation to provide comments on the proposed interagency guidance on third-party relationships: risk management, as this is an important matter. If left unclarified, this guidance may read as jargon that is challenging to put into practice. This is important to resolve, to ensure the soundness of the American banking industry and consumer protections. Please consider this information and these recommendations as you finalize the guidance.

Sincerely,
Rocio Baeza
CEO and Founder
CyberSecurityBase
rocio@cybersecuritybase.com

You are invited to view a supplementary video recording on this matter at:
https://cybersecuritybase.com/thirdpartyrisk