State of North Carolina
OFFICE OF THE COMMISSIONER OF BANKS

PAT MCCRORY
GOVERNOR

RAY GRACE
COMMISSIONER OF BANKS

Information Technology Questionnaire – Addendum to the Money Transmitter Application

General Instructions

Please answer the following information technology program questions as part of the money transmitters application process. The majority of the questions require only a response of "Yes," "No" or "NA" (non-applicable). However, you are encouraged to expand on or clarify any response as needed, directly below each question in the "Comments" section. Please do not leave responses blank, and provide any supporting documentation.

General comments for consideration may be under the "Clarifying or Additional Comments for Consideration" section.

The questionnaire must be signed by an executive officer in front of a notary, attesting to the accuracy and completeness for all responses.

Questions

1. Has management designed and implemented an information security program (ISP) to protect customer and other non-public information? ☐ Yes ☐ No ☐ NA

   If yes, does the ISP include:
   a. written policies and procedures? ☐ Yes ☐ No ☐ NA
   b. employee training provisions? ☐ Yes ☐ No ☐ NA
   c. ongoing monitoring provisions? ☐ Yes ☐ No ☐ NA

   d. provisions for testing the effectiveness of key controls, such as through audit engagements, penetration tests, vulnerability assessments, internal control reviews, etc.? ☐ Yes ☐ No ☐ NA
   e. provisions for evaluating and adjusting the program as needed? ☐ Yes ☐ No ☐ NA

Comments:

2. Has management performed a risk analysis to identify and assess the risks to customer information in each relevant area of business operations, including IT?
☐ Yes ☐ No ☐ NA

   If yes, does the risk analysis evaluate the effectiveness of current safeguards or controls?
☐ Yes ☐ No ☐ NA

   Comments:

3. Does management rely on external service providers to provide business functions that allow access to customer information? ☐ Yes ☐ No ☐ NA

   If yes, does management:
   a. select vendors that can maintain appropriate safeguards over customer information?
☐ Yes ☐ No ☐ NA
   b. contractually require the vendors to maintain appropriate safeguards?
☐ Yes ☐ No ☐ NA
   c. oversee the vendor's handling of customer information? ☐ Yes ☐ No ☐ NA

   Comments:

4. Has management implemented an internal audit program? ☐ Yes ☐ No ☐ NA

   If yes, does the scope of the internal audit program include:
   a. network security? ☐ Yes ☐ No ☐ NA
   b. IT general controls? ☐ Yes ☐ No ☐ NA
   c. penetration testing? ☐ Yes ☐ No ☐ NA
   d. application development policies and procedures? ☐ Yes ☐ No ☐ NA
   e. disaster recovery/business continuity planning? ☐ Yes ☐ No ☐ NA
   f. information security program? ☐ Yes ☐ No ☐ NA
   g. compliance with applicable safeguarding customer information regulations?
☐ Yes ☐ No ☐ NA

Please list below the details of any audits performed in the last 24 months.

Audit Type	Audit Date	Audit Firm Name	Audit Firm City, State

Comments:

5. Does the applicant develop or support custom software that is used for conducting daily business activities? ☐ Yes ☐ No ☐ NA

   If yes, are development/support activities:
   a. based on written policies and procedures? ☐ Yes ☐ No ☐ NA
   b. properly segregated? ☐ Yes ☐ No ☐ NA
   c. based on secure program coding practices that meet industry standards? ☐ Yes ☐ No ☐ NA
   d. subject to independent review and testing to ensure there are no security and integrity issues prior to migration into production environments? ☐ Yes ☐ No ☐ NA

   Comments:

6. Does the applicant conduct business through Internet channels such as a web portal or through mobile applications? ☐ Yes ☐ No ☐ NA

   If yes, have all Internet-facing applications been subject to web application security testing, including penetration testing? ☐ Yes ☐ No ☐ NA

   Comments:

7. Does the application rely on agents or branches to conduct business activities? ☐ Yes ☐ No ☐ NA

   If yes, is agent access to the applicant's systems:
   a. granted based on defined security policies/procedures? ☐ Yes ☐ No ☐ NA
   b. based on two or more factor authentication? ☐ Yes ☐ No ☐ NA
   c. logged and routinely monitored? ☐ Yes ☐ No ☐ NA

   Comments:

8. Has management implemented a comprehensive, enterprise-wide, disaster recovery/business continuity program (DR/BCP) for continuation of business operations in the event of an emergency? ☐ Yes ☐ No ☐ NA

   If yes, does the DR/BCP contain:
   a. defined roles and responsibilities? ☐ Yes ☐ No ☐ NA
   b. written recovery procedures)? ☐ Yes ☐ No ☐ NA
   c. business impact analysis? ☐ Yes ☐ No ☐ NA
   d. provisions for offsite storage of critical data? ☐ Yes ☐ No ☐ NA
   e. testing requirements, which include documentation of the scope, frequency, effectiveness, and lessons learned from any DR/BCP test performed?

   Comments:

9. Has management implemented an incident response plan/program? ☐ Yes ☐ No ☐ NA

   If yes, does the plan contain procedures for:
   a. assessing the nature and scope of the incident, including any customer information systems that may have been compromised? ☐ Yes ☐ No ☐ NA
   b. containing and controlling the incident to prevent further compromise?
   c. appropriate law enforcement and regulatory notifications? ☐ Yes ☐ No ☐ NA
   d. preserving records and other evidence? ☐ Yes ☐ No ☐ NA
   e. customer notification when warranted? ☐ Yes ☐ No ☐ NA
   f. periodic employee awareness training? ☐ Yes ☐ No ☐ NA

   Comments:

Clarifying or Additional Comments for Consideration

Certification

I certify that the information provided in this questionnaire is correct to the best of my knowledge and belief (must be signed by executive officer).

NAME (print or type): _____
TITLE (print or type): _____
SIGNATURE: _____ DATE: _____

STATE OF _____, COUNTY OF _____

Sworn to and subscribed before me this _____ day of _____, in the year _____, and I hereby certify that I am not an officer or director of this bank/trust company.

_____
Notary Public

My commission expires: _____ (Notary Seal)