b4,b8

ATTACHMENT

Please provide the following items for the proposed crypto-related activity with b4,b8 and any other similar relationships.

- Overview of the relationship, including the role of all third parties, the bank's role, and how customers interact with third parties and the bank as it relates to this product/service.
- Description of the digital wallet, the bank's role in managing the digital wallet, all third party roles in managing the wallet, and all information security analysis related to the wallet.
- Customer journey screens for the relationship, including the digital wallet.
- Description of the 'virtual ledger' and its purpose / function. Note: "virtual ledger" was referred to in the draft Addendum to the Program Account Agreement.
- Data flows.
- Funds flows, including a list, titling, and purpose of all accounts at the bank to manage the activity.
- Provide analysis on deposit volatility and how such deposits are considered in liquidity risk management functions including:
  - Concentration risk limits;
  - Key risk indicators outlining the minimum level of highly liquid assets held against crypto-related deposits; and
  - Any other supporting metrics to assist with understanding how management assesses and manages the overall risk related to digital asset related deposit accounts.
- Incentive compensation plans and agreements.
- All policies and procedures (including any drafts if not yet final) governing these activities.
- Committee minutes for all committees with oversight responsibilities related to this activity.
- Wire Transfer Policy.
- Enterprise-wide crypto and country risk assessments.
- Risk assessment for the activity and third parties.
- Feasibility and profitability analysis.
- All contracts related to the activity, including all schedules and amendments.
- Signature cards for all omnibus, For Benefit Of, or other deposit accounts used for b4,b8 and any other similar relationship.
- Actual and projected volume of deposits, transaction activity, and users.
- Due diligence performed on b4,b8 and any other third parties, including all supporting documentation.
- List approved states/countries for b4,b8-related activity. Provide implemented controls for prohibited states/countries.
- Documentation for quality control, testing, and on-going oversight of b4,b8 Include procedures for handling requests to b4,b8 for information on specific transaction activity.
- Copies of all contracts associated with b4,b8 relationship and any other third parties.
- Legal review of all contracts.
- Monthly deposit volumes and monthly payment volumes (by payment rail, e.g., wire and ACH) and associated return rates.
- Wire logs reflecting incoming and outgoing transactions since activity inception.
- Two most recent payment risk monitoring reports utilized by management and relevant

b4,b8

committees.AML/CFT

- Listing of software systems/programs that will be used for AML/CFT compliance.
- System settings for automated systems or programs used for the Customer Identification Program (CIP), OFAC sanctions monitoring, and suspicious activity monitoring.
  - Description of process/controls for revising settings.
- Due diligence of system/program and support for settings selected, if automated systems or programs are used, for CIP, OFAC, and suspicious activity monitoring.
- Account agreements for this type of customer relationship.
- Auditor access to the bank's suspicious activity monitoring system used to monitor b4,b8 transactions.

- **Fraud Prevention**
  - Description of fraud detection systems, mechanisms, and processes.
  - Description of fraud loss mitigation processes.

- **Consumer Protection**
  - Description of any fees that will be charged to consumers related to the activity, and how they will be calculated.
  - Consumer agreements, disclosures, or other terms and conditions related to the activities provided by or through the bank and by third parties (draft or proposed).
  - Marketing materials, press releases, internal scripts, educational materials, and any other publicly distributed information related to the activity (draft or proposed).
  - Policies and procedures that will govern the crypto-related activities, including those related to consumer compliance and complaint resolution.
  - Internal training materials related to the activities.
  - Provide documentation of any internal or external analysis, including legal opinions, conducted to determine whether the digital asset firm disclosures and any related third party's account agreements are accurate as it relates to the availability of FDIC pass through deposit insurance.

- **Application Programming Interface**
  - Please provide narrative detailing APIs calling critical bank systems. For each of these APIs, please provide the following:
    - Name of API and/or product calling critical bank systems. If API calls are external, please also list the whitelisted domain(s) making the calls.
    - What critical systems is this API calling?
    - What function/process is this API facilitating?
    - Is this API internally developed, developed on behalf of the bank by a third party, or developed by a contracted service provider/fintech?
  - Please provide narrative around API controls implemented. At a minimum, please address:
    - What authentication standard is used to authenticate incoming API calls?
    - What systems/interfaces are used to whitelist domains to allow incoming API calls to critical bank systems? If not provided elsewhere, provide a brief overview of user access controls over those systems.

b4,b8

- Preventative control – Once a domain is whitelisted, how does the bank restrict API call activity to only the bank systems and fields the end product needs?
    - For example, a budgeting tool for consumers needs to read account balance but not send payments related API calls such as wire or ACH.
- Preventative Control – How does the bank restrict API call activity to specific fields or call type.
    - For example, that same consumer budgeting tool needs to read account balance in the core processing system, but not write to account balance. Further, it may need to read some fields but likely not fields like TIN/SSN.
- Detective Control – Please provide narrative around the scope of API logging, aggregation, and review at the bank. Are API logs being ingested into SIEM and alerts crafted for anomalous API calls, such as the above example of the budgeting software tool trying to write to account balance instead of read or call the wrong bank systems/functions?
- Please provide an inventory of all internet domains built and managed by the bank. Provide brief narrative of the purpose of each domain and whether it is facilitating APIs.