Summary of the OCC's Paycheck Protection Program Listening Session on Fraud Identification and Solutions held on April 20, 2020

The Office of the Comptroller of the Currency (OCC) hosted a listening session[1] on April 20, 2020, to discuss issues and potential solutions relating to the Paycheck Protection Program (PPP). The overarching purpose of this listening session was to maximize the PPP's chance of success by identifying positive solutions to implementation problems that banks had raised to the OCC. During this listening session, participants described issues and potential solutions[2] relating to the identification of fraud,[3] such as loan stacking and misrepresentations in the loan application and forgiveness processes. The topic of fraud identification was chosen given concerns raised about the potential for fraud associated with a large program like the PPP.

The discussion began with an introduction by the OCC's Senior Deputy Comptroller and Chief Operating Officer, Brian Brooks, who noted that one of the roles of the OCC's Office of Innovation is to convene parties for discussion and information sharing. The purpose of today's call was to facilitate discussions between lenders and nonbank solution providers about ways to better detect fraud on loans originated under the PPP. The goal of the session was to explore not only the possible challenges associated with fraud detection, but also the potential solutions, including technology-related products and processes. The OCC's Chief Innovation Officer, Beth Knickerbocker, also emphasized that a key goal of the OCC is to support responsible innovation and that the information and possible solutions identified by this listening session could be broadly applicable to more efficient and effective management of prudent small business lending in the future.

Following these remarks, participants were asked to discuss the possible types of fraud that may occur during the loan application or loan forgiveness process.

Several participants noted concerns related to the potential for synthetic identity fraud. In general, synthetic identity fraud occurs when some element of a real identity is used, and fictional information is added to build a credible identity. Participants indicated that solely relying on an employer identification number (EIN) and/or taxpayer identification number (TIN) to verify a small business increases the risk of fraud as different EIN/TINs could be substituted to obtain multiple loans to one small business. Participants also indicated that loan applications, even for existing customers, often have different phone numbers and addresses. Therefore, if businesses are closed, applicants may be using personal addresses and phone numbers which also increases the risk of fraud in the form of account takeover.

Participants raised additional concerns and the need for robust mechanisms to identify fraudulent applications. For example, the need for systems that can quickly and effectively identify the submission of multiple applications by changing the identification numbers. Loan stacking, the process by which a

---

[1] Listening sessions are used to inform the OCC and participants about emerging topics, issues, or concerns of stakeholders such as banks and nonbanks, including financial technology companies. The goal of listening sessions is to encourage an open dialogue between participants. Listening sessions are not intended to result in a group consensus on recommendations to guide OCC policy or regulation.

[2] The OCC does not endorse any particular solutions, companies, or technologies.

[3] Borrowers must provide documentation to verify their eligibility for the program. See Paycheck Protection Program Application, Small Business Administration Form 2483 (3/20). Also, see Paycheck Protection Program Loans Frequently Asked Questions, dated April 8, 2020.

borrower obtains multiple loans from multiple institutions, was also discussed. Finally, participants raised questions about independent contractors and self-employed individuals, such as lawyers or contract workers who are paid through multiple businesses and how to ensure these businesses do not exceed the total salary thresholds in the PPP.

Participants were then asked to describe potential technology-related solutions to help reduce the risk of fraud in the PPP. One participant suggested the development of multiple verification factors to build out a company "fingerprint" using unique characteristics. This could be used to verify the authenticity of a small business and help prevent synthetic identity fraud. A participant offered as a solution the use of third-party products that access multiple data sources such as phone numbers, state license and registration information and other available information to perform real time verification of business owners. Another participant mentioned the use of third-party payroll providers to verify information. One participant indicated that some online fintechs use selfies with a government issued ID to verify customers when the transaction is not face-to-face. Participants suggested that a similar method could be used to verify applicants applying on behalf of small businesses.

Participants also discussed leveraging different technologies including data aggregation, blockchain, and application programming interfaces (APIs) to assist with fraud detection. Data aggregation could be leveraged to allow lenders to verify information without accessing it and blockchain technology could be used to document multiple attributes to uniquely identify small businesses. One participant indicated an API based system could be set up to prevent loan stacking, and artificial intelligence/machine learning could be used to identify large-scale fraud patterns. Participants also discussed KYC solutions designed for small businesses and using chat bots to collect required documentation and to assist applicants through the loan process.

In addition, participants suggested expanding the data types used to validate small businesses to assist with fraud identification. Many participants are running new fraud identification tools and processes in parallel, rather than integrating new technology solutions or processes to detect fraud with plans to integrate them in the future.

Ms. Knickerbocker provided closing remarks and thanked participants for the informative discussion.

###