Ex. 5 – Guidance Document from SBA and U.S. Secret Service titled "Paycheck Protection Program—Application Fraud Indicators," dated March 19, 2021

U.S. Secret Service
Office of Investigations

U.S. Small Business Administration
Office of Inspector General

March 19, 2021

Paycheck Protection Program—Application Fraud Indicators

Financial institutions (FI) have advised the U.S. Small Business Administration Office of Inspector General (SBA-OIG) and the U.S. Secret Service of several commonalities discovered on thousands of Paycheck Protection Program (PPP) loan applications.

PPP Application Fraud Indicators

In March 2021, SBA-OIG and Secret Service were notified of the below common fraud indicators, appearing individually or in combination, that occurred across thousands of PPP applications.

- Green Dot Bank provided as the deposit account—Green Dot believes that it is high risk for PPP funding to be deposited into a direct deposit consumer account and that such deposits should be rejected
- Noticeably photo-shopped state-issued identification cards (ID) or driver licenses (DL) with blurry backgrounds
- Multiple applicants utilizing ID/DL with the same photo, but altered information
- Bank statements with little or no activity listed
- Multiple applicants utilizing identical bank statements with altered account names
- Blank or illegible supporting documents
- Multiple applications originating from the same IP address and/or physical address
- Identical formatting of tax documentation provided, including text font
- Requests for same loan amounts, to the penny
- Digitally voided checks provided by applicants

Suspicious Activity Report (SAR) Filing

SAR reporting, in conjunction with effective implementation of due diligence requirements by FIs, is crucial to identifying and stopping financial crimes, including those related to the COVID-19 pandemic. FIs should provide all pertinent and available information in the SAR and narrative.

Guidance on Returning Funds

If a Receiving Depository Financial Institution (RDFI) has determined to return an Automated Clearing House (ACH) credit entry because the RDFI believes the entry was initiated due to fraud, the RDFI should select the Return Reason Code that most closely approximates the reason for the return. The following examples may be acceptable options:

- ✓ R03 (No Account/Unable to Locate Account)

- ✓ R17 (File Record Edit Criteria/Entry with Invalid Account Number Initiated Under Questionable Circumstances), which requires "QUESTIONABLE" to be inserted in the first twelve positions of the Addenda Record
- ✓ R23 (Credit Entry Refused by Receiver)

RDFIs can make a business decision to return these credit entries outside of the standard return timeframe. Due to the extraordinary circumstances and the lenders' desire to recoup the funds, it is unlikely that the return of credits will be dishonored as untimely.

Partial return of funds can be handled outside of the ACH Network (e.g., with a wire transfer or an official check), or with a new ACH credit entry agreed to by both institutions to return the available amount. The ODFI should, or be prepared to, offer a Letter of Indemnity to the RDFI.

Guidance on Searching ACH Codes

PPP funds are disbursed through third-party FIs. There are instances when a participating lender will receive the PPP application, but the loan disbursement will be sent from another ODFI. The RDFI can determine where the funds were disbursed by querying the ODFI's ACH routing number or the first 8 numbers of the trace number through the Federal Reserve Bank E-Payments Routing Directory, which provides basic routing information for Fedwire® Funds Service, Fedwire Securities Service, and FedACH® transactions. This information is synchronized with the Federal Reserve FedACH and Fedwire databases daily and is provided solely as a service to financial institutions and other authorized users to help process and settle their transactions efficiently.

Guidance on Reporting to Law Enforcement

To most effectively counter PPP fraud and other financial crimes, the Secret Service continues partnering with the U.S. Department of the Treasury and the Treasury Financial Crimes Enforcement Network (FinCEN), SBA-OIG, the U.S. Department of Justice, United States Attorney Office (USAO) COVID-19 task forces, state, local, tribal, and territorial (SLTT) law enforcement agencies, state prosecutors, various Inspector Generals, other Federal law enforcement agencies, and foreign law enforcement.

To report fraudulent activity, contact your local U.S. Secret Service field office Cyber Fraud Task Force (CFTF).

FIs may also report fraud, waste, abuse, or mismanagement of federal funds involving SBA programs, operations, or personnel to the SBA-OIG Hotline at 800-767-0385 or online.

Information contained in this alert was compiled from the following sources:

U.S. Secret Service Office of Investigations

U.S. Small Business Administration Office of Inspector General

U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN)