



SBA Information Notice

TO: Depository Financial Institutions and All
SBA Employees

CONTROL NO.: 5000-20037

EFFECTIVE: July 21, 2020

SUBJECT: Guidance Regarding Identification and
Reporting of Suspicious Activity in the COVID-19
EIDL Loan Program

The purpose of this notice is to provide a brief overview of COVID-19 assistance available under SBA's Economic Injury Disaster Loan (EIDL) Program, including both advances (grants) and direct loans, and to alert depository financial institutions to the potential for suspicious activity related to COVID-19 EIDL funds deposited into business or personal accounts. This Notice also provides points of contact at SBA for depository financial institutions to report suspicious activity in the COVID-19 EIDL loan program.

The SBA EIDL direct loan program, administered by SBA's Office of Disaster Assistance (ODA), offers long-term, low-interest loans to eligible small businesses, private non-profit organizations, and agricultural businesses that have suffered substantial economic injury as a result of a declared disaster. SBA has issued COVID-19 disaster declarations for all U.S. states and territories. Eligible applicants must apply directly to SBA using the online SBA COVID-19 EIDL portal (available at <https://www.sba.gov/funding-programs/disaster-assistance/coronavirus-covid-19>). For the COVID-19 disaster, Section 1110 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) (P.L. 116-136) authorized SBA to provide advances of up to \$10,000 to applicants that applied for COVID-19 EIDL loans and self-certified as to eligibility, while the applicants await processing of their EIDL loan applications. The COVID-19 EIDL advance is a grant that must be used for general business purposes.

When SBA disburses an EIDL advance or an EIDL loan to an applicant or borrower, all proceeds are deposited ONLY into the verified Financial Institution account belonging to the eligible applicant or borrower. For purposes of the EIDL program, a verified Financial Institution account is a depository institution account using the Employer Identification Number (EIN) or Social Security Number (SSN) entered by the applicant or borrower in the EIDL loan

PAGE 1 of 3

EXPIRES: 7-1-21

SBA Form 1353.3 (4-93) MS Word Edition; previous editions obsolete

Must be accompanied by SBA Form 58

application. No third-party service provider is authorized by SBA to receive EIDL advance or EIDL loan funds on behalf of an applicant or borrower.

SBA has become aware of certain suspicious activity associated with the COVID-19 EIDL loan program. SBA is requesting the assistance of depository financial institutions in identifying and reporting suspicious activity to SBA as well as to other appropriate regulatory agencies.

Examples of COVID-19 EIDL suspicious activity include, but are not limited to, the following:

- Use of stolen identities or EIN or SSN numbers to qualify for the EIDL advance or EIDL loan.
- Purported businesses, including front or shell companies, lacking an indicia of operating presence or history, receiving EIDL advances or EIDL loans.
- Applicants working with third parties to obtain EIDL advances or EIDL loans in exchange for keeping a percentage of the funds.
- Account holders that are victims of social engineering schemes and may not know that the source of the funds is an EIDL advance or EIDL loan.
- A customer advises a financial institution that the customer received a COVID-19 EIDL ACH deposit from “*SBAD TREAS 310*” and “*Origin No. 10103615*” into their account, but did not apply for a COVID-19 EIDL loan.
- The financial institution is aware that it previously denied a customer’s Paycheck Protection Program loan after applying the institution’s risk-based Bank Secrecy Act compliance protocols.

Additionally, depository financial institutions are encouraged to examine the following transactions more closely to determine if they constitute COVID-19 EIDL suspicious activity:

- A customer not known to be a small business, sole proprietor, or independent contractor receives a lump sum COVID-19 EIDL ACH deposit from “*SBAD TREAS 310*” and “*Origin No. 10103615*” into a personal account.
- A new customer opens an account and shortly thereafter receives a COVID-19 EIDL ACH lump sum deposit from “*SBAD TREAS 310*” and “*Origin No. 10103615*”.
- A single account receives multiple EIDL advance or multiple EIDL loan deposits.

Depository financial institutions are also directed to the COVID-19 webpage maintained by the Financial Crimes Enforcement Network (FinCEN) at <https://www.fincen.gov/coronavirus>. This webpage, which is updated on an ongoing basis, provides notices and advisories to depository financial institutions regarding illicit financial activity related to COVID-19.

If a depository financial institution detects suspicious activity in a customer's account relating to COVID-19 EIDL advance or loan deposits, the institution should follow the protocols of the institution's compliance division and the institution's state or federal regulator(s), including filing a Suspicious Activity Report with FinCEN as appropriate. Additionally, SBA requests that depository financial institutions report suspicious activity associated with the COVID-19 EIDL loan program to SBA's Office of Inspector General through one of the following methods:

Telephone: OIG Hotline at 1-800-767-0385

Email: OIGHotline@sba.gov

Website: Complete the on-line OIG Complaint Submission Form at <https://www.sba.gov/office-of-inspector-general>

SBA point of contact for questions regarding suspicious activity associated with the COVID-19 EIDL loan program is: eidl.ach.inquiries@sba.gov.

SBA appreciates the cooperation and diligence of depository financial institutions in identifying and reporting suspicious activity associated with the COVID-19 EIDL loan program.

William M. Manger
Chief of Staff