Accuracy Counts: Filing Complete and Accurate SARs and Program Specific Red Flags Related to Covid-19 Criminal or Fraudulent Activity

09/30/2020

On September 29, 2020, at the 19th Annual AML & Anti-Financial Crime Conference, Financial Crimes Enforcement Network ("FinCEN") Director Kenneth Blanco reported over 91,000 suspicious activity reports ("SARs") have been filed related to Covid-19 criminal and fraudulent activity. These 91,000 reports have resulted in the initiation of 57 prosecutions so far and leave over $100,000,000 in tax payer dollars in question. The magnitude of this level of fraudulent activity indicates the fervency with which financial institutions need to continue to approach this issue – specifically in the accuracy of filling out an SAR narrative and recognizing the red flags that trigger the reports. Director Blanco reiterated multiple times the importance of properly completing the SAR to ensure the report is directed to the appropriate governmental investigation team as specialized teams have been created to review fraudulent activity related to the different various relief programs created in response to the pandemic.

SAR form reminders

As a reminder, using the FinCEN requested information within the SAR form increases the speed with which your financial institution will receive assistance. Below are the following recommendations provided by FinCEN for completing SARs.

- Include the key term "COVID19 FIN-2020-A002" in SAR field 2 and write the narrative so that it indicates a connection between the suspicious activity being reported and the activities highlighted in FinCEN advisories,
- Select SAR field 34(z) (Fraud – other) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and COVID-19,
- Include the type of fraud and/or name of the scam or product (e.g., Product Fraud – non-delivery scam) in SAR field 34(z), and
- Refer to FinCEN's May 18, 2020 Notice Related to the Coronavirus Disease 2019 (COVID-19), which contains information regarding reporting COVID-19-related crime and reminds financial institutions of certain BSA obligations.

Recognizing Red Flags

Coupled with a strong AML/OFAC/BSA policy, arming your customer facing staff with red flags related to various relief programs is the best way to assist your financial institution in catching the fraud and reducing potential criminal fines and liability for compliance failures.

Economic Injury Disaster Loans ("EIDL")

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 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.
- A customer receives a COVID-19 EIDL ACH deposit after the financial institution previously denied the customer's Paycheck Protection Program (PPP) loan application, particularly where the financial institution identified inaccurate or incomplete information in the customer's PPP loan application.

Paycheck Protection Program ("PPP")

PPP fraud can occur at either the application or forgiveness stage and each stage may present different red flags for your staff to identify.

Application Stage Red Flags

- Failure to provide appropriate documentation supporting employee history,
- A customer states they are unable to provide corporate documents or secretary of state filings supporting the existence of an incorporated business,
- An applicants may inflate payroll to qualify for a higher loan amount (loan amounts are based on 2.5x the cost of payroll),
- Multiple applications are submitted from eligible businesses using phished information,
- A customer has no history of conducting business with the financial institution or has no online presence related to their business.

Forgiveness Stage Red Flags

- A businesses must provide proof of how loan funds are used to determine how much of the loan will be eligible for forgiveness and thus the failure to provide such documentation indicates funds were misappropriated,
- The loan funds have been funneled into an account with a different name than the applicant or business (this may also be a red flag at the application stage),
- A borrowers may try to manipulate funds or documents to meet forgiveness eligibility.

As a reminder, financial institutions that assisted new customers in applying for PPP loans should revisit those customers and ensure they have collected the following information from all natural persons with a 20% or greater ownership stake in the applicant business to satisfy applicable BSA and FinCEN regulations governing the collection of beneficial ownership information:

- Owner name,
- Title,
- Ownership %,
- TIN,
- Address, and
- Date of birth

Unemployment Benefit Program

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

- employees who return to work but continue to collect unemployment insurance benefits,
- mass or batch uploads of employee wage records,
- fictitious employer schemes or “two-sided” schemes,
- unemployment insurance benefits that are deposited into common bank accounts,
- claimants filing under synthetic or stolen identities,
- claimants filing for inmates, deceased persons, or out-of-state applicants; or,
- fictitious businesses that hire and then layoff “employees” in order to file unemployment insurance claims.