

The Small Business Administration (SBA) offers some guidance regarding how small business lending scams related to COVID-19 work and what activities should raise a red flag warning you that you should suspect fraud.

Grant Fraud Schemes

The SBA does not contact individual businesses on either 7(a) loans or disaster loans/grants. If anyone contacts you claiming to be from the SBA, you should immediately suspect fraud and don't share any personal or business information with them.

Loan Fraud Schemes

If you are contacted by anyone promising you an SBA loan approval but requires payment up front or offers a high-interest bridge loan in the interim, you should immediately suspect fraud. The SBA does not guarantee approval before an application is submitted and reviewed.

Any attempt to charge borrower fees in excess of 3% is likely fraud. The SBA limits fees a broker can charge to 3% for loans of \$50,000 or less and 2% for loans of \$50,000 to \$1 million. Loans over \$1 million will include an additional 1/4% or 2-1/4%.

Phishing Schemes

If you are in the process of applying for an SBA loan and receive an email asking for Personally Identifiable Information (PII), make sure the referenced application number is consistent with the actual application number.

Don't assume that something with the SBA logo must be legitimate. These phishing attacks may be attempts to obtain your PII to gain access to your bank accounts or to install ransomware/malware on your computer.

Make sure any email correspondence claiming to be from the SBA is from the SBA. Every email from the SBA will come from accounts ending in sba.gov. The presence of the SBA logo on a webpage does not guarantee it is endorsed by the SBA. Verify and cross-reference any information you receive with information available at www.sba.gov.