U.S. Small Business Administration

Rapid Reference Guide

Below are the various "INFO" messages that may be seen when processing files in the RER system. "INFO" messages are generated based on established business rules and require further review by a loan officer. These items must be addressed and mitigated appropriately. Below are the actions to be taken in response to each of the "INFO" messages that may appear on deals in process.

Before decisioning any deals, review the Notes for information pertaining to the file.

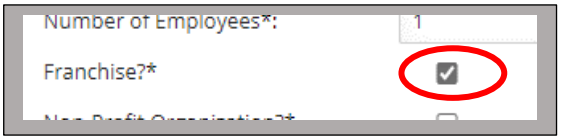
INFO: Advance amount sent to client
INFO: If loan is funded, applicant will receive advance of $XXXX
EIDL Advance amount ranging from $1,000 - $10,000, based on $1,000 per employee.

Action To Take:

No action necessary. **EIDL Advances are no longer available, as all appropriations for this program have been allocated.**

INFO: Applicant indicated they are a Franchise:

Results when the Applicant indicates the business is a Franchise.



Action To Take:

- Check SBA's franchise directory, in addition to the supplemental ***SBA Franchise Team ODA-Only Brands*** list located on the DIG to determine if the applicant's brand is listed.

[redacted]

SBA FRANCHISE IDENTIFIER CODE	BRAND	MEETS FTC DEFINITION?	IS AN ADDENDUM NEEDED?	SBA ADDENDUM - Form 2462	SBA NEGOTIATED ADDENDUM	SBA FRANCHISE IDENTIFIER CODE Start Date	NOTES
S3456	A Mother's Touch Movers	Y	Y	Y	N	09/05/2018	When the real estate where the franchise business is located will secure the SBA-guaranteed loan, the Collateral Assignment of Lease may not be executed.

Rapid Fraud ALERTS

These are meant for internal use only. Do not discuss specific details with applicants.



Loan Officer Action:

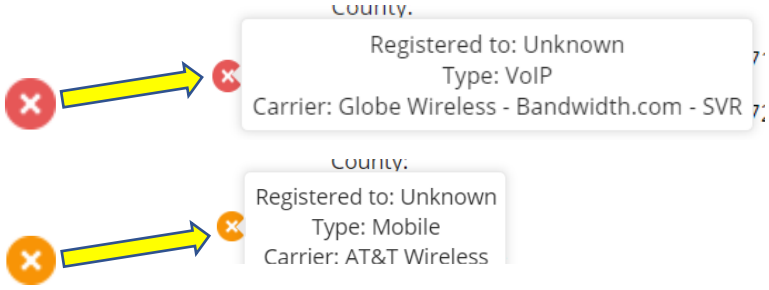
1. High risk IP address – The computer or mobile device may have been reported to be used in fraudulent activity by other institutions, not an automatic decline. Must telephone contact applicant to confirm PII information. Inquire about the alert to update Notes. If everything is correct = **Approve the loan.** If unable to contact or phone has been disconnected = **Decline the loan (If fraud or identity theft is suspected/reported, notify PDC's Fraud Review Team at [redacted]@sba.gov or [redacted]@sba.gov)**
2. Suspicious online behavior – The portal may have been accessed from multiple devices, the applicant may have used a phone or tablet or the data altogether has possibly been used fraudulently online. Owner associated with fraud online or we detected attempts to bypass our fraud checks and security measures. Telephone the applicant to ask some verification PII questions and discuss how they have accessed the portal, document in NOTES. Verbal request or send an email to obtain a copy of their valid identification. **If not received within 7 days = Decline the loan (If fraud or identity theft is suspected/reported, notify PDC's Fraud Review Team at [redacted]@sba.gov or [redacted]@sba.gov)**
3. Fraud found on related deal(s) – Must review each Related Deal that is identified as potential fraud to determine what is the potential fraud and how it relates to the applicant directly or indirectly. Document these findings in Notes.
4. Large number of applications with other providers – Owner information used in a high volume of applications with multiple institutions within a short period of time. Often indicates stolen PII. Telephone the applicant to determine if he has applied with other sources. Confirm the source and if funds were received as this could be a duplication of benefit. Add your comments to the notes = **Approve the loan**
5. Large number of applications for this program – Often indicates attempt to get multiple funding (several in succession) or use of different false information. **Could also be an owner with multiple businesses**. Review each application to determine if they are duplicates. Mark accordingly. **(If fraud or identity theft is suspected/reported, notify PDC's IG Liaisons at [redacted]@sba.gov or [redacted]@sba.gov)**
6. Client information failed validation – Owner information could not be validated by data provider. Indicates red flags or discrepancies (information doesn't go together, person may have been listed as deceased, etc.). Telephone the owner/principal who failed the validation. Ask verification PII questions to confirm their identity. Send an email to obtain a copy of a valid government issued photo ID to further verify identity**. If not received within 7 days or if unable to confirm identity = Decline the loan**
7. Failed online identity verification – Telephone the owner/principal who failed the online identity verification. Ask verification PII questions to confirm their identity. May need to send an email to obtain a copy of a valid government issued photo ID to

further verify identity**. If not received within 7 days or if unable to confirm identity = Decline the loan**

8. Client location is international – Applicant accessing software from a non-U.S. location. Accessed application from another country. Generally higher fraud rates from international traffic. Determine if the applicant business has a physical presence in a declared county. If not, **Decline** for no physical presence.
9. Client device(s) associated with fraud – Applicant possibly is accessing their Rapid loan through an unsecured WIFI at any public establishment. Telephone the applicant to inquire as to how they are accessing their loan, update Notes. Make sure to confirm PII that applicant matches application. May need to send an email to obtain a copy of their government issued identification. No other Alerts or Info messages move forward with approval.

OTHER FRAUD INDICATORS TO MONITOR

VOIP phone number or phone number not associated with business or owner – Often used by nefarious organizations to mask their true phone number and locations. Name associated with the telephone number does not match the applicant or business entity. **Also used by legitimate businesses**. Look at the totality of the potential issues with inconsistent information associated with Fraud.
Telephone the applicant, confirm phone number – **Approve**



Email has not passed validation – Incorrect or fake email may suggest business may not be legitimate. Telephone contact with applicant to obtain correct valid email address. Email address must be correct and accurate to insure loan documents are emailed out through DocuSign correctly.