CITADEL
SERVICING CORPORATION

Fraud Detection Policy and Process Overview

DataVerify Fraud Protection

Overview:

Citadel Servicing Corporation ("CSC") has adopted the use of Fraud Detection Tools such as "FraudGuard" and "DataVerify". These tools are used to help identify and authenticate the borrower, and all participants to the loan transaction, Verify the information supplied by the borrower in their application, and assess the value of the property to be purchased of refinanced.

The Fraud Detection Tool is utilized at the initial underwriting review and the final funding review prior to the closing of the loan. This sequencing of running the tool twice in the origination loan lifecycle was structured so that all pertinent information in the initial application packet is reviewed at submission and all other inclusionary information related to participators involved in the transaction are reviewed prior to the closing of the loan.

All of these tools provide an alert summary that outlines any potential findings and their associated risk factor. All "high" risk factors are address through the underwriting process via conditioning of the loan and not through the tool providers website.

> Note, certain risk factors that are not relevant to the loan will not addressed. For example, social security number alerts on foreign national borrowers (who have no social security number) will not be addressed (This is due to configuration limitations).

All fraud detection tool related conditions must be satisfied prior to the closing of the loan.

Processes and Responsibilities by Departments:

Loan Set-Up:

The Loan Set-up team is responsible for running DataVerify on every loan submitted to Citadel Servicing Corporation ("CSC"). DataVerify should be run as soon as the loan file is submitted and a file is created in BytePro. A printout of the report must be stored in DocVelocity at this time for review by the Underwriter.

Underwriting:

The Underwriter is responsible for reviewing the DataVerify findings in DocVelocity. Any valid conditions/alerts raised in the DataVerify report must have conditions created in BytePro which will not allow the loan to proceed to the closing department until they are satisfied.

Upon receipt of relevant information, the Underwriter is responsible for the review, validation, and clearance of all Fraud Tool associated conditions.

> *Escalation:*
>
> Findings which cannot be cleared or are deemed to have required additional review should be sent to the compliance department via email at CSCQC@CitadelServicing.com.

Transaction Management:

The Transaction manager is responsible for requesting and retrieving any additional information required by the underwriter as conditioned in BytePro.

Closing/Funding Department:

All conditions related to the Fraud Detection Tool or any other fraud concerns must have been cleared by Underwriting or the Compliance department prior to proceeding with the closing/funding of the loan.

If new findings exist on the second run of the Fraud Detection Tool which have not been addressed by the Underwriter, a condition must be created in BytePro. When the Underwriter has reviewed and cleared the new findings the condition should be cleared and the file is clear to proceed with the funding process.

Escalation:

Findings which cannot be cleared or are deemed to have required additional review should be sent to the compliance department via email at CSCQC@CitadelServicing.com.

QC/Compliance:

Any findings which require additional research or have a compliance facet to them will be escalated by the Underwriter through the CSCQC inbox.

The QC Auditor is responsible for completing thorough research into all aspects of the escalated finding and determining, with the assistance of the Compliance Officer, whether the finding presents a valid risk to the loan. If a finding cannot be cleared the loan will not be cleared to proceed.

Any questions related to this process should be directed to the Compliance Department via email CSCQC@CitadelServicing.com.