201-808-7000
885 Teaneck Rd
Teaneck NJ 07666
crossriver.com

OCT Fraud Submission Protocol

COMPLIANCE

201-808-7000
885 Teaneck Rd
Teaneck NJ 07666
crossriver.com

Software Disclaimer

All OCT Fraud Submission Protocol software and systems, and the information and materials contained or made available in this Compliance are provided on an "as-is," "as available" basis without warranty of any kind. Neither Cross River Bank (the Bank) nor any of its current or future affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries make any warranties regarding the use, operation or performance of software and systems utilized for OCT Fraud Submission Protocol, or to the content of material set forth herein, whether express or implied, and the Bank and affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries expressly disclaim all implied warranties, including any warranty of merchantability or fitness for a particular purpose. The Bank has no liability with respect to any software or system or for any inaccurate or incomplete information or claims that may result from reliance on such information contained herein. Neither the Bank nor any of its affiliates or subsidiaries or the employees, successors or assigns of it or its affiliates or subsidiaries shall be liable for, and hereby expressly disclaim any, liabilities, and warranties with respect to other third-party components of material contained herein.

201-808-7000
885 Teaneck Rd, Teaneck NJ 07666
crossriver.com

Table of Contents

201-808-7000
885 Teaneck Rd, Teaneck NJ 07666
crossriver.com

Abstract

Beginning on October 13, 2023, Visa will require Acquirers to report suspected OCT fraud i.e., the use of OCTs to distribute fraudulently obtained funds.

This requirement is intended to enhance ecosystem visibility into fraud trends, assist Issuers in identifying accounts opened by fraudsters through access to Acquirer reports of suspected OCT fraud, and support the development of new client tools and services to mitigate the risks of OCT fraud, such as OCT fraud risk scoring tools.

Reporting Requirement

1. Send an email to cardpaymentops-disputes@crossriver.com including at least the following information:
    a. **Date of the Transaction(s)**:
    b. **Transaction Amount**:
    c. **Customer Name**:
    d. **Transaction Request ID (TransactionRequestId)**:
    Include the unique identifier associated with the transaction request. This helps in tracking and verifying the transaction.
    e. **Fraud Type:** (as identified in Appendix C)
    f. **CAID**: (not required, providing this item can enhance our review process)
    Card Acceptor ID, is a code or identifier used to designate the merchant or business that accepted a card payment in each transaction.

2. In accordance with the thresholds outlined in Appendix A "Incident Report Submission Summary", send an Incident Report, if warranted, to **unusualactivityreferrals@crossriverbank.com.** Use the Incident Report form in Appendix B.

Appendix A - Incident Report Submission Summary

The Partner must escalate the following unusual activity to CRB via an Incident Report (IR):

- The following unusual activity needs to be escalated to Cross River via an Incident Report (IR):
    - Criminal violations involving insider abuse in any amount.
    - Criminal violations aggregating $5,000 or more when a suspect can be identified.
    - Criminal violations aggregating $25,000 or more regardless of a potential suspect.
    - Transactions aggregating $5,000 or more, if the Partner knows, suspects, or has reason to suspect that the transaction:
        - May involve potential money laundering or other illegal activity.
        - Is designed to evade the BSA or its implementing regulations; or,
        - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the Partner knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Partner should maintain a documented IR process i.e., notifying the Bank of potentially unusual or Suspicious Activity. Escalations need to be made within 5 days of detecting unusual activity by completing a CRB IR and sending it to **unusualactivityreferrals@crossriver.com**. Incident report submission must include relevant supporting documentation.

Appendix B - Incident Report Template

INCIDENT REPORT	
Date reported to CRB:	Name of bank partner:
Name and address of applicant:	Account number and date of application:
Dollar amount requested or obtained:	Amount of financial loss: (if applicable)
Name of suspect: (if identified)	Are there any application(s) linked to this application? Yes: ___ or No: ___ If yes, have you provided all relevant details for the linked application(s) below? Yes: ___ or No: ___
PLEASE BE AS DETAILED AS POSSIBLE IN THE NARRATIVE, AND ATTACH ALL SUPPORTING DOCUMENTATION.	
Submitted By: Submitted Date: Telephone:	X_____ _ Employee Signature
FOR BSA USE ONLY: Approved By: Determination Date:	X_____ _ Employee Signature

Appendix C - Fraud Types

Fraud Type	Definition
Fraud Type B – Account or Credential Takeover	• Fraud resulting from fraudsters taking over an account or credentials from a legitimate client. • Examples: • Fraudulent use of the account holder's digital wallet via stolen user credentials (i.e., mobile passcode, wallet login information). • Fraudulent use of card data and PII to circumvent the issuer's authentication process and enable provisioning of the payment card onto a mobile device/digital wallet, which is subsequently used for fraudulent purchases.
Fraud Type C – Merchant Misrepresentation:	• Fraud resulting from a merchant deliberately misleading the account holder. • Examples: • A merchant fraudulently selling items that are not as they seem or substandard, charging more than anticipated or for a longer term, or charging for a service that the consumer can get for free through another channel for the purpose of conducting fraudulent activity.
Fraud Type D – Manipulation of Account Holder:	• Fraud resulting from a merchant manipulating an account holder into completing what they believe to be a legitimate transaction. • Examples: • Account holder manipulated into sending funds to a fraudulent beneficiary when the sender believes they will gain fictitious riches or help an individual in distress, a struggling business, or to pay medical fees. • A fraudster contacting the sender to impersonate a known supplier, trusted organization, or business to request a change of payment details for a transaction or to request a payment to a fraudulent account.
Fraud type 6 – Fraudulent use of account number:	Account number used in the non-face-to-face environment (card-not- present), including mail order, telephone order, recurring payments, installments, and e-commerce (internet) transactions. Examples: • A user loads funds to a wallet from stolen card credentials, and then sends an OCT to a card that they legitimately own.
Fraud type 9 – Counterfeit:	The transaction involved an unissued or invalid BIN.
Fraud type 5 – Miscellaneous:	The transaction is determined to be fraudulent but does not fall into any of the other categories listed above. Examples: • Multiple draft imprints obtained unlawfully from a legitimate card. • Unauthorized alterations to a sales draft.