Codego Fraud policy

Purpose

The purpose of this policy is to define Codego's official stance on fraud prevention, detection, and response. This policy is designed to protect the company and its customers from fraudulent activities by establishing clear procedures for identifying, managing, and addressing fraud at all levels of the organization.

Scope

This policy applies to all Codego employees, contractors, third-party vendors, and customers. It encompasses any and all types of fraud that could impact Codego's operations or reputation, whether originating internally or externally. Everyone in the organization is expected to adhere to the procedures outlined in this policy.

Types of fraud addressed

- Codego is committed to addressing multiple types of fraud, including but not limited to:
- External fraud such as phishing, identity theft, unauthorized transactions, and account takeovers.
- Internal fraud including embezzlement, misuse of company assets, and collusion with external fraudsters.
- Financial crimes such as money laundering, terrorism financing, and the use of stolen payment credentials.

Responsibilities

The Fraud Department at Codego takes the lead in detecting and managing fraud risks. Compliance teams ensure that all fraud-related processes comply with local and international regulations. Senior management is responsible for establishing a culture of zero tolerance towards fraud, and all employees are encouraged to report suspicious activity through defined internal channels.

Prevention and detection mechanisms

Codego leverages several tools and techniques to detect and prevent fraudulent activity. Among these are third-party solutions such as Seon, which offers advanced fraud monitoring and detection capabilities. Codego also employs strong KYC processes, including Enhanced Due Diligence (EDD) and regular customer reviews. These systems work together to ensure real-time detection of suspicious transactions and mitigate the risk of fraud.

Reporting and investigation

Any suspected or actual fraud must be reported immediately to the Risk and Fraud Department, either internally or via external customer reports. The Fraud Department is responsible for investigating these reports, gathering evidence, and determining whether fraud has occurred.

Consequences of fraudulent activity

Employees, third parties, or customers found engaging in fraudulent activity will face severe consequences. This may include termination of employment or contract, legal action, and being reported to law enforcement authorities. Codego takes a zero-tolerance stance on fraud and will take all necessary steps to ensure that fraudulent actors are held accountable.

Fraud and financial crime risk assessment

Introduction

Codego is firmly committed to combating fraud and financial crime by maintaining a robust and comprehensive framework for identifying, preventing, and responding to potential risks. As the financial landscape evolves, Codego actively seeks to adapt to emerging threats through continuous monitoring and a proactive approach to security.

Fraud risk assessment overview

Codego has identified several key areas where fraud risk is prevalent, both internally and externally. Internal risks include possible employee collusion or insider fraud, while external risks involve fraudulent third parties, malicious actors engaging in phishing attacks, and account takeovers. The company regularly conducts in-depth risk assessments to adapt its processes and security measures.

External fraud risks

Codego is particularly vigilant against external fraud, including phishing attacks, identity theft, and account takeovers. Malicious actors often target customers through social engineering and other deceptive practices. With its global customer base, Codego is especially cautious about fraudulent activities originating from external partners or third-party vendors.

Mitigation measures

To mitigate these risks, Codego employs Seon, a leading third-party tool for fraud prevention, detection, and management. Seon leverages a robust set of security rules, real-time data, and machine learning algorithms to monitor transactions and flag suspicious behavior. In addition, Codego implements stringent KYC (Know Your Customer) and Enhanced Due Diligence (EDD) processes. All customers must undergo thorough verification, including providing a source of funds to ensure compliance with anti-money laundering (AML) regulations.

Conclusion

Codego remains dedicated to maintaining high standards in fraud detection and prevention through continuous updates to its systems, training programs, and partnerships with industry-leading security firms. The company also emphasizes ongoing training and awareness programs for staff to stay ahead of potential threats. Regular reviews and audits ensure that the security framework remains effective and responsive to new challenges.

Procedure for returning funds to fraud victims

Purpose

The purpose of this procedure is to outline the steps Codego takes to ensure the timely and transparent return of funds to victims of fraud. Codego is committed to protecting its customers and ensuring that, in the event of fraud, the recovery process is as efficient and clear as possible.

Process

Fraud detection and reporting: Fraudulent activity is first detected through internal monitoring systems (such as Seon) or by a direct report from the customer. Once identified, the fraudulent transaction is flagged, and immediate action is taken to freeze the transaction or account involved. Customers are encouraged to report any suspicious activity through dedicated channels, including phone, email, or the online platform.

Verification and investigation

Codego verifies the legitimacy of the fraud claim through a rigorous investigation process. All flagged transactions are thoroughly examined using transaction data, customer identification, IP addresses, and other relevant information. Depending on the complexity, investigations may take a few days to several weeks. Throughout this process, Codego follows KYC and AML guidelines to ensure compliance and proper identification of fraud patterns.

Collaboration with banks and payment providers

Codego works closely with third-party financial institutions, banks, and payment processors to retrieve funds involved in fraudulent transactions. This collaboration is essential, especially when transactions span multiple jurisdictions or involve international payment systems. Codego adheres to all legal and regulatory requirements in these interactions to ensure swift and legitimate action.

Refund

Codego applies strict eligibility criteria when determining if funds can be refunded. If the fraud claim is verified and the funds have not been irreversibly transferred, the victim will be reimbursed through their original payment method. In cases of authorized fraud (such as Authorized Push Payment fraud, confirmed fraud (confirmed stolen funds or identity), additional investigation may be required to establish liability before a refund is processed.

Customer communication

Throughout the process, Codego ensures that fraud victims are regularly updated on the investigation's progress. Dedicated customer service representatives provide clear communication on the expected timeline for resolution and any required actions on the part of the customer. Transparency is maintained at every stage to ensure the customer remains informed and reassured.

Fraud metrics

Customer-level fraud metrics

1. **Account Takeover (ATO) attempts:**
    - Number of account takeover attempts detected.
    - Frequency of failed login attempts from unusual IP addresses or devices.
    - Number of accounts locked due to suspicious activity.
2. **Know Your Customer (KYC) verification failures:**
    - Number and percentage of customers failing initial KYC checks.
    - Number of customers flagged during Enhanced Due Diligence (EDD).
    - Time taken to complete KYC/EDD processes.
3. **Suspicious account activity:**
    - Accounts with abnormal activity (sudden large transactions, frequent transfers).
    - Frequency of changes to sensitive information (address, email, phone number).
    - Number of flagged customer accounts due to changes in transaction patterns.

4. **Customer fraud risk scores:**
    - Risk scores based on behavior, geolocation, device fingerprinting, etc.
    - Percentage of customers flagged as high-risk.
    - Distribution of customers across different risk score ranges.
5. **Chargeback and refund ratios:**
    - Number of chargebacks initiated by customers.
    - Percentage of transactions resulting in a chargeback.
    - Average value of chargebacks per customer.
6. **Customer support fraud reports:**
    - Number of fraud reports made by customers to customer support.
    - Time taken to resolve reported fraud cases.
    - Number of reports resulting in confirmed fraud.

Transaction-level fraud metrics

1. **Fraudulent transaction volume and value:**
    - Number and total value of fraudulent transactions detected.
    - Percentage of fraudulent transactions compared to total transactions.
    - Rate of fraudulent transaction attempts blocked in real-time.
2. **Transaction monitoring alerts:**
    - Number of suspicious transactions flagged for manual review.
    - Number of transactions escalated due to fraud risk.
    - False positive rate (legitimate transactions flagged as fraud).
3. **Transaction velocity monitoring:**
    - Number of transactions performed within a short period.
    - Number of flagged transactions due to unusual frequency.
    - Average value of flagged high-velocity transactions.
4. **Geolocation and IP anomalies:**
    - Transactions originating from high-risk geographies or IP addresses.
    - Number of flagged transactions due to geolocation mismatches.
    - Percentage of cross-border transactions flagged as suspicious.
5. **Payment method risk:**
    - Fraud rates per payment method (credit card, bank transfer, etc.).
    - Number of flagged transactions involving new or unverified payment methods.
    - Success rate of fraud attempts using high-risk payment methods.
6. **Transaction reversal metrics:**
    - Number of transaction reversals due to confirmed fraud.
    - Percentage of reversed transactions successfully recovered.

    - Time taken to reverse fraudulent transactions.

Additional metrics:

- **Time to detect and resolve fraud:**
    - Average time to detect a fraudulent transaction.
    - Average time to fully resolve a fraud case (from detection to closure).
    - Average duration between fraud detection and customer notification.
- **Fraud prevention efficacy:**
    - Accuracy of fraud detection algorithms (Seon) based on false positives/negatives.
    - Impact of fraud prevention measures on legitimate transactions (e.g., decline rates).
    - Percentage of transactions manually reviewed vs. automated detections.

Fraud management and reporting process

Fraud investigation process

Codego initiates the fraud investigation process as soon as suspicious transactions are flagged by internal systems or reported by customers. Seon, Codego's fraud detection tool, plays a crucial role in identifying unusual patterns, unauthorized access, and potentially fraudulent activities. Once a transaction is flagged, the Fraud Department gathers relevant data, including transaction history, customer information, and technical details such as IP addresses, to assess the legitimacy of the transaction. Investigations are handled promptly to minimize financial loss and mitigate any further risks.

Blocking and reporting of fraudulent transactions

When a transaction is confirmed to be suspicious, immediate action is taken to freeze or block the funds associated with the transaction. Codego uses an automated process to block high-risk accounts, preventing further fraudulent activities. Once the transaction is blocked, Codego's internal team files necessary reports to regulatory authorities as part of Anti-Money Laundering (AML) and Know Your Customer (KYC) compliance. The fraud cases may also be reported to law enforcement when required by legal obligations.

Returning funds

Codego follows strict criteria to determine whether funds can be returned to the victims of fraud. If the fraud claim is verified and it is confirmed that the victim had no role in facilitating the fraudulent activity, Codego works with its financial partners to reverse or return the funds. If the funds have already been transferred out, Codego collaborates with international banking institutions and payment providers to retrieve the stolen money. In cases where recovery is impossible, Codego informs the victim and may provide compensation based on the severity and nature of the fraud.

Tracking and reporting

Codego employs a comprehensive fraud management system to continuously track fraud cases from initiation to resolution. Each case is logged with detailed information, including transaction data, customer interactions, and investigation outcomes. The system enables Codego to analyze fraud trends and improve detection mechanisms over time. Monthly and quarterly fraud reports are generated for senior management and compliance teams to ensure that the company remains informed about current threats and emerging risks. These reports are also shared with regulators as part of Codego's commitment to transparency and compliance.

Marianna Luisi
Chief Executive Officer, Codego
Date: September 12, 2024