EXTERNAL FRAUD PREVENTION AND RISK MANAGEMENT POLICY

DECEMBER 2021

INDEX

1 – Framework

This Policy sets out general principles, responsibilities and rules on External Fraud Prevention and Risk Management at Caixa Geral de Depósitos (hereinafter referred to as "CGD" or "the Bank").

In order to protect its reputation and meet legal and regulatory obligations, CGD adopts responsible measures to minimize external fraud risk and other related offences throughout its organization.

Accordingly, external fraud risks are internally defined and adequate internal controls are implemented in a timely manner to prevent, detect and respond to fraud and other related infractions.

The adopted Policy is supported by a control environment, which includes a program where the Bank's top management sets an example and where training and communication actions are promoted to raise employee awareness, as well as to create an ethical and open culture.

External Fraud Prevention and Risk Management Policy provides guidelines on the fraud identification, the controls to be implemented to prevent and detect fraud and the steps to be completed in order to build a robust response to protect the interests of the Bank and its customers.

2 – Fraud Definition

Fraud can be defined as the practice of an illicit, intentional and deceivable action, punishable by Law, perpetrated by a fraudster with the aim of deceiving or harming a person or an organization, for his or her own or a third party's benefit, to avoid a certain obligation or to cause losses for a certain organization.

External Fraud refers to potential losses following CGD customers and third parties (other stakeholders, excluding employees) activities with fraudulent intent.

In this sense, External Fraud occurs when the acts defined in the Fraud concept are perpetrated by people or entities outside the CGD Group.

3 – Dimensions of the Fraud Prevention and Management Process

Fraud Prevention and Management Process is depicted by three dimensions:

i) Planning and Prevention;

ii) Detection, Diagnosis, Analysis and Resolution; and

iii) Control and Evaluation.

3.1 PLANNING AND PREVENTION

CGD is structured in accordance with de best practices of Fraud Risk Prevention ("FRP") in order to promote a robust risk management and control culture. Roles and responsibilities of the respective areas have been defined and forums where the 'FRP' is analyzed and assessed on a regular basis are organized.

3.1.1 Onboarding

When establishing a business relationship with a new customer or with a new counterparty, the Bank performs the procedures already recommended in the Know Your Customer ("KYC") requirements regarding Prevention of Money Laundering and Terrorist Financing ("AML/CFT").

These KYC procedures, in addition to preventing Money Laundering and Countering the Financing of Terrorism ("ML/FT") risks, also mitigate exposure to financial, regulatory and/or reputational risks.

3.1.2 Authentication

In order to prevent fraud, reputational and regulatory risks, as well as data breaches or theft, the Bank has implemented controls to minimize the risk of unauthorized access to customer accounts and transactions.

Accordingly, the authentication methods in place at CGD are based on a risk-based approach, whereby more robust authentication measures (strong authentication) are applied to operations of higher risk.

3.1.3 Cybersecurity

CGD, through its institutional website, www.cgd.pt, permanently publishes security alerts and recommendations on protection against the risks of computer fraud ("phishing" and others), in order to promote safe use of the internet and the services of payment through electronic means.

Additionally, Caixa's homebanking services have permanent monitoring systems that prevent and detect fraud attempts.

The use of these fraud prevention and verification systems allows for the identification of suspicious activities, helping to protect the accounts and interests of CGD customers.

3.1.4 Vulnerable Customers

Under the risk-based approach, the Bank identifies potentially vulnerable customers in the fraud risk management framework.

A potentially vulnerable customer is someone who, due to personal circumstances, is especially susceptible to fraud threats, particularly if the Bank fails to act with appropriate level of care.

Potentially vulnerable customers include:

i) elderly customers;

ii) customers with mental / physical disabilities; and,

iii) marginalized customers.

The approach considers

i) the possible indicators of vulnerability; and,

ii) how the different areas inadvertently avoid excluding customers or placing barriers that impact their ability to use the products and services offered by the Bank.

3.1.5 Customer awareness

CGD provides awareness-raising materials on FRP to its customers and other counterparties through its institutional website and other publications, sharing information on fraud issues, such as trends, campaigns and alerts on recurring situations.

3.2 DETECTION, DIAGNOSIS, ANALYSIS AND RESOLUTION

Under the risk-based approach, CGD documents the identification of potential fraud practices and suspicious activities. The approach used includes the processes, technologies and systems used to detect suspected fraud activities.

In order to detect fraud practices and suspicious activities, CGD has implemented controls, which are proportional to the level of fraud risk identified.

All detected fraud cases are managed in line with the internal processes defined under the FRP and reviewed considering all available information, in order to determine whether if it is considered a potential fraud incident. If so, the cases with suspected fraud are forwarded to a higher level of review, along with the supporting documentation.

CGD has an audit trail record of all cases of analyzed fraud, as well as of the decisions and actions taken in order to mitigate the associated risk, making it possible to report periodically ~~on~~ the cases identified.

Within the scope of the Fraud Risk Prevention activity, if there are suspicions of external fraud incidents and if applicable, the Bank reports the incident to the authorities.

Additionally, the Bank maintains an effective relationship with the authorities, which facilitates the sharing of information, support in responding to fraud attacks and better cooperation in the investigation of external fraud cases. All the information requests of the police authorities are responded within the established time frame.

3.3 MONITORING AND EVALUATION

3.3.1 Risk Assessment

CGD periodically conducts a business risk assessment regarding external fraud.

This assessment, in addition to determining the inherent risks of external fraud, makes it possible to determine the effectiveness of the controls in place, as well as to identify opportunities for improvement.

CGD has zero tolerance for external fraud incidents.

The risk assessment includes, at a minimum, the:

i) identification of the risks in the business area based on its structure, products, services and distribution channels;

ii) identification of processes and controls in place to mitigate the risks;

iii) identification of gaps or weaknesses in the control structure facing the risks.

3.3.2 Evaluation of effectiveness, continuous improvement and reporting

Departments and areas assigned to Fraud Risk Prevention conduct control tests to assess the suitability, design and operational effectiveness of their fraud procedures, systems and controls.

These tests are risk-based and tailored to the specific risks of each Fraud Risk Prevention unit, with a greater focus on transactions, customer vulnerabilities and activities that have a higher risk of fraud.

When incidents of fraud are detected, CGD conducts root-cause analysis regarding the review of alerts, resolution and customer response. The results and conclusions of these analysis support changes to the controls or procedures and risk assessments carried out.

Fraud metrics are an essential tool to quantify and report the nature of the fraud risks to which CGD is exposed to. Periodic and timely collection and analysis of the information are essential for effective management, reporting and supervision of fraud risks.

A report is prepared on a quarterly basis reporting to the Board the main activities developed within the scope of external fraud prevention and management.

3.3.3 Records

In line with good practices regarding the archiving of documentation, CGD keeps documentation on External Fraud Risk Prevention and Management for a minimum period of 7 years.

CGD establishes documented procedures, systems and controls in order to ensure the conservation and appropriate access to the documents listed above.

All documents must be legible, auditable and retrievable and are compliant with all applicable legislation regarding confidentiality, secrecy and data protection.

Luís Saraiva Martins
Head of Compliance