Insight Series on the Central Bank of Ireland's Consultation Paper on the Consumer Protection Code
Insight 3: Financial Abuse (Frauds and Scams)

Overview

As set out in our *Initial Observations on the Central Bank of Ireland's Consumer Protection Code Consultation Paper*, the Central Bank of Ireland (the "**Central Bank**") has proposed a revised structure for the Consumer Protection Code (the "**CPC**") under CP158 - Consultation Paper on the Consumer Protection Code ("**CP158**") comprising:

(i) The Central Bank Reform Act 2010 (Section 17A) (Standards for Business) Regulations, (the "**Standards for Business Regulations**");

(ii) The Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Conduct of Business Regulations) (the "**Conduct of Business Regulations**");

(iii) The Supporting Guidance on Securing Customers' Interests; and

(iv) The Supporting Guidance on Protecting Consumers in Vulnerable Circumstances;

(together the "**Revised Code**").

Our most recent insight discussed the new Standards for Business - Securing Customers Interests, which regulated financial service providers ("**RFSPs**") must adhere to in their dealings with consumers in Ireland (actual and potential).

This insight will focus on the new Standard for Business relating to Financial Abuse (frauds and scams).

The Central Bank believes that RFSPs have a responsibility to work collectively to ensure that the financial system is resilient and responsive to the threat of frauds and scams. The Standard for Business Regulations therefore propose a new standard for business which aims to ensure that RFSPs are taking the necessary steps to protect the system and their customers from financial abuse.

Scope

This new Standard for Business applies to all RFSPs, other than those providing MiFID services and crowdfunding services (for which there are equivalent regimes in EU legislation) and credit unions ("**Excluded Firms**"), in respect of both current and potential customers.

The Conduct of Business Regulations, set out additional obligations on RFSPs which aim to prevent frauds and scams occurring and provide additional protections for Consumers in Vulnerable Circumstances. The new Standard for Business to protect customers against financial abuse is intrinsically linked to the specific obligations on RFSPs when dealing with Consumers in Vulnerable Circumstances. These obligations will be considered in further detail in a later insight on Consumers in Vulnerable Circumstances.

Financial Abuse - New Standard for Business

The Central Bank is seeking to modernise the CPC and given the prevalence of frauds and scams, a new Standard for Business will be introduced, aimed at the protection of customers against financial abuse through frauds and scams. This update is in line with the G20/OECD High-Level Principles on Financial Consumer Protection which seek to ensure that information, control and protection mechanisms are appropriately developed and implemented by oversight authorities and financial services providers and with a high degree of certainty protect consumers' deposits, savings, and other similar financial assets, including against fraud, scams, misappropriation or other misuses. . The Central Bank notes that RFSPs have a responsibility to work collectively to ensure that the system is resilient and responsive to the ever-evolving threat of frauds and scams, and the continuing problems associated with elder financial abuse.

The new Standard for Business requires an RFSP to control and manage its affairs and systems to counter the risks to customers of financial abuse. Certain RFSPs will already be subject to rules seeking to prevent fraud, for example, under payment services legislation, certain payment service providers are subject to strong-customer-authentification rules. RFSPs will also have obligations arising under anti-money-laundering legislation, for example, to identify and report suspicious transactions which could have a fraudulent element. This new Standard for Business seeks to complement these existing rules, requiring firms to safeguard against frauds and scams by adequately controlling and managing their affairs and systems. RFSPs will therefore be required to take a holistic view of their products and business with a view to preventing financial abuse.

New Definition

A new definition of 'financial abuse' is proposed to explain the circumstances that the new Standard for Business will apply to. Financial Abuse will mean:

(a) the wrongful or unauthorised taking, withholding, appropriation, or use of a customer's money, assets or property;

(b) any act or omission by a person, including through the use of a power of attorney, guardianship, or any other authority regarding a customer, to –

(i) obtain control, through deception, intimidation or undue influence, over the customer's money, assets or property, or

(ii) wrongfully interfere with or deny the customer's ownership, use, benefit or possession of the customer's money, assets or property.

Supporting Standards

The supporting standards aim to provide greater clarity and outline in further detail the obligations on RFSPs to mitigate the risk to customers of financial abuse, ensuring that RFSPs control and manage their affairs and systems to counter the risks to customers of financial abuse by:

(i) Putting **reasonable systems** and controls in place for the provision of their financial services, to mitigate the risk to customers of financial abuse;

(ii) **Ongoing Monitoring** of trends in financial abuse (relevant to customers or the sector) and in particular potential vulnerabilities in the customer process and distribution channels;

(iii) Ensuring **appropriate escalation** processes are in place where there is an increased risk to customers of financial abuse; and

(iv) **Communicating clearly** to customers (i) any digital frauds or deception to the firm or the sector of which the RFSP is aware, (ii) the supports available to customers and (iii) actions that customers can take in the event of financial abuse, in relation to the RFSP's product or service.

Notification Requirement

The supporting standards propose a new notification requirement, requiring RFSPs to *"notify customers through clear and timely communication of any digital frauds or deception connected to its affairs, or specifically relevant to the sector in which the regulated financial services provider is operating, and of which it is aware"*.

This notification requirement is aligned with the obligations on RFSPs to secure customers' interests and inform effectively and consistently with the outcomes-focused approach that the Central Bank is seeking to achieve under the Revised Code. Further detail on this can be found in our previous insight on Securing Customers' Interests and our next insight Informing Effectively.

Impact on RFSPs

The New Standard for Business Regulations will require RFSPs to examine their existing systems and controls, internal monitoring of financial abuse and vulnerabilities in their services along with their communication processes to ensure compliance with the new requirements. This review should be appropriately documented to evidence how RFSPs meet this new Standard for Business. RFSPs must then update their internal processes and procedures to ensure they are controlling and managing their affairs and systems to counter the risk of financial abuse to customers. This will likely require RFSPs to conduct a root and branch review as part of the implementation of the Revised Code to comply with the new Standard for Business.

It is recognised at EU level that further improvements to the EU legislative framework are needed to address fraudulent transactions, particularly so-called "authorised push payment" fraud. This arises where a person is deceived into transferring funds to another person or funds are transferred for a purpose which was fraudulently misrepresented. There are a number of proposals under active consideration and the Central Bank will continue to engage with these developments. In this regard, new rules are proposed under draft legislation seeking to amend the second Payment Services Directive and introduce a directly-effective suite of payment service regulations. The prevention and detection of frauds and scams are also being considered domestically under the National Payments Strategy; it will then be determined whether a domestic solution is also required alongside the EU proposals.

Upcoming

Keep an eye on Matheson's Insights page for our next Insight in this series.

For any queries on this Insight or any aspect of the CPC, please do not hesitate to contact Darren Maher, Gráinne Callanan, Elaine Long, Joe Beashel, Ian O'Mara, Niamh Mulholland or your usual Financial Institutions Group contact at Matheson

Darren Maher
Partner
T +353 1 232 2398
E darren.maher@matheson.com

Gráinne Callanan
Partner
T +353 1 232 8211
E grainne.callanan@matheson.com

Elaine Long
Partner
T +353 1 232 2694
E elaine.long@matheson.com

Joe Beashel
Partner
T +353 1 232 2101
M +44 7933 502322
M + 353 86 824 4444
E joe.beashel@matheson.com

Ian O'Mara
Partner
T +353 1 232 2874
E ian.o'mara@matheson.com

Niamh Mulholland
Partner
T +353 1 232 2061
E niamh.mulholland@matheson.com