ANNEX II: INFORMATION REQUIRED FROM APPLICANTS FOR AUTHORISATION AS ACCOUNT INFORMATION SERVICE PROVIDERS (AISPs)

INTRODUCTION

This Annex supplements paragraph 34 of FIR/01. This Annex applies to applicants for authorisation as AISPs.

PROGRAMME OF OPERATIONS

The Programme of Operations should contain the following:

a) a description of the account information service that is intended to be provided, including an explanation of how the applicant determined that the activity fits the definition of account information services as defined in Article 2 of the Act;

b) a declaration from the applicant that they will not enter at any time into possession of funds;

c) a description of the provision of the account information service including:

   i. draft contracts between all the parties involved, if applicable;
   ii. terms and conditions of the provision of the account information services;
   iii. processing times;

d) the estimated number of different premises from which the applicant intends to provide the services, if applicable;

e) a description of any ancillary services to the account information service, if applicable;

f) a declaration of whether or not the applicant intends to provide account information services in another EU Member State or another country once registered;

g) an indication of whether the applicant intends, for the next three years, to provide, or already provides, business activities other than account information services as referred to in paragraphs (a) to (c) of paragraph 3 of the Second

Schedule to the Act, including a description of the type and expected volume of the activities;

h) the information specified in Annex IV of the Rules on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee where the applicant intends to provide only service listed under paragraph 2(h) of the Second Schedule to the Act (AIS).

BUSINESS PLAN

The business plan should contain:

a) a marketing plan consisting of:
   i. an analysis of the company's competitive position in the payment market segment concerned;
   ii. a description of the payment service users, marketing materials and distribution channels;

b) certified annual accounts for the previous three years, if available, or a summary of the financial situation for those applicants that have not yet produced annual accounts;

c) a forecast budget calculation for the first three financial years that demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures that allow the applicant to operate soundly; it should include:
   i. an income statement and balance-sheet forecast, including target scenarios and stress scenarios as well as their base assumptions, such as volume and value of transactions, number of clients, pricing, average amount per transaction, expected increase in profitability threshold;
   ii. explanations of the main lines of income and expenses, the financial debts and the capital assets;
   iii. a diagram and detailed breakdown of the estimated cash flows for the next three years.

MONITORING SECURITY INCIDENTS AND SECURITY RELATED CUSTOMER COMPLAINTS

Provide a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, which should contain:

a) organisational measures and tools for the prevention of fraud;

b) details of the individual(s) and bodies responsible for assisting customers in cases of fraud, technical issues and/or claim management;

c) reporting lines in cases of fraud;

d) the contact point for customers, including a name and email address;

e) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including notification of major incidents to the Authority, in line with the EBA guidelines on incident reporting;

f) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks.

SENSITIVE PAYMENT DATA

Provide a description of the process in place to file, monitor, track or restrict access to sensitive payment data consisting of:

a) a description of the flows of data classified as sensitive payment data in the context of the AISP's business model;

b) the procedures in place to authorise access to sensitive payment data;

c) a description of the monitoring tool;

d) the access right policy, detailing access to all relevant infrastructure components and systems, including databases and back-up infrastructures;

e) a description of how the collected data is filed;

f) the expected internal and/or external use of the collected data, including by counterparties;

g) the IT system and technical security measures that have been implemented including encryption and/or tokenisation;

h) identification of the individuals, bodies and/or committees with access to the sensitive payment data;

i) an explanation of how breaches will be detected and addressed;

j) an annual internal control programme in relation to the safety of the IT systems.

BUSINESS CONTINUITY

Provide a description of business continuity arrangements consisting of the following:

a) a business impact analysis, including the business processes and recovery objectives, such as recovery time objectives, recovery point objectives and protected assets;

b) the identification of the back-up site, access to IT infrastructure, and the key software and data to recover from a disaster or disruption;

c) an explanation of how the applicant will deal with significant continuity events and disruptions, such as the failure of key systems; the loss of key data; the inaccessibility of the premises; and the loss of key persons;

d) the frequency with which the applicant intends to test the business continuity and disaster recovery plans, including how the results of the testing will be recorded.

SECURITY POLICY DOCUMENT

The Applicant should provide a security policy document should contain the following information:

a) a detailed risk assessment of the payment service(s) the applicant intends to provide, which should include risks of fraud and the security control and mitigation measures taken to adequately protect payment service users against the risks identified;

b) a description of the IT systems, which should include:

i. the architecture of the systems and their network elements;
ii. the business IT systems supporting the business activities provided, such as the applicant's website, the risk and fraud management engine, and customer accounting;
iii. the support IT systems used for the organisation and administration of the AISP, such as accounting, legal reporting systems, staff management, customer relationship management, e-mail servers and internal file servers;
iv. information on whether those systems are already used by the AISP or its group, and the estimated date of implementation, if applicable;

c) the type of authorised connections from outside, such as with partners, service providers, entities of the group and employees working remotely, including the rationale for such connections;

d) for each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the applicant will have over such access as well as the nature and frequency of each control, such as technical versus organisational; preventative versus detective; and real-time

monitoring versus regular reviews, such as the use of an active directory separate from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus systems and logs;

e) the logical security measures and mechanisms that govern the internal access to IT systems, which should include:

   i. the technical and organisational nature and frequency of each measure, such as whether it is preventative or detective and whether or not it is carried out in real time;
   ii. how the issue of client environment segregation is dealt with in cases where the applicant's IT resources are shared;

f) the physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

g) the security of the payment processes, which should include:
   i. the customer authentication procedure used for both consultative and transactional access;
   ii. an explanation of how safe delivery to the legitimate payment service user and the integrity of authentication factors, such as hardware tokens and mobile applications, are ensured, at the time of both initial enrolment and renewal;
   iii. a description of the systems and procedures that the applicant has in place for transaction analysis and the identification of suspicious or unusual transactions;

h) a detailed risk assessment in relation to its payment services, including fraud, with a link to the control and mitigation measures explained in the application file, demonstrating that the risks are addressed;

i) a list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalised, an estimated date for their finalisation.

STRUCTURAL ORGANISATION

If the applicant is a natural person the description of the structural organisation should contain:

a) an overall forecast of the staff numbers for the next three years;

b) a description of relevant operational outsourcing arrangements consisting of:
   i. the identity and geographical location of the outsourcing provider;

ii. the identity of the persons within the AISP that are responsible for each of the outsourced activities;
iii. a detailed description of the outsourced activities and their main characteristics;

c) a copy of draft outsourcing agreements;

d) a list of all natural or legal persons that have close links with the applicant, indicating their identities and the nature of those links.

If the applicant is a legal person, the description of the structural organisation of its undertaking should contain the following information:

a) a detailed organisational chart, showing each division, department or similar structural separation, including the name of the person(s) responsible, in particular those in charge of internal control functions; the chart should be accompanied by a description of the functions and responsibilities of each division, department or similar structural separation;

b) an overall forecast of the staff numbers for the next three years;

c) a description of the relevant outsourcing arrangements consisting of:

i. the identity and geographical location of the outsourcing provider;
ii. the identities of the persons within the AISP that are responsible for each of the outsourced activities;
iii. a detailed description of the outsourced activities and its main characteristics;

d) a copy of draft outsourcing agreements;

e) if applicable, a description of the use of branches and agents, including:

i. a mapping of the off-site and on-site checks that the applicant intends to perform of branches and agents;
ii. The IT systems, processes and infrastructures that are used by the applicant's agents to perform activities on behalf of the applicant;
iii. in the case of agents, the selection policy, monitoring procedures and agents' training and, where available, the draft terms of engagement;

f) a list of all natural or legal persons that have close links with the applicant, indicating their identities and the nature of those links.

GOVERNANCE ARRANGEMENTS AND INTERNAL CONTROL MECHANISMS

The Applicant should include a description of the governance arrangements and internal control mechanisms consisting of:

a) a mapping of the risks identified by the applicant, including the type of risks and the procedures the applicant will put in place to assess and prevent such risks;

b) the different procedures to carry out periodical and permanent controls including the frequency and the human resources allocated;

c) the accounting procedures by which the applicant will record and report its financial information;

d) the identity of the person(s) responsible for the internal control functions, including for periodic, permanent and compliance control, as well as an up-to-date curriculum vitae;

e) the identity of any auditor that is not a statutory auditor pursuant to Directive 2006/43/EC;

f) the composition of the management body and, if applicable, of any other oversight body or committee;

g) a description of the way outsourced functions are monitored and controlled so as to avoid an impairment in the quality of the applicant's internal controls;

h) a description of the way any agents and branches are monitored and controlled within the framework of the applicant's internal controls;

i) where the applicant is the subsidiary of a regulated entity in another EU Member State, a description of the group governance.

PROFESSIONAL INDEMNITY INSURANCE OR COMPARABLE GUARANTEE

As evidence of a professional indemnity insurance or comparable guarantee that is compliant with Annex IV of FIR/01 and Article 5(1B) of the Act, the applicant for the provision of AIS should provide the following information:

a) an insurance contract or other equivalent document confirming the existence of professional indemnity insurance or a comparable guarantee, with a cover amount that is compliant with the referred Annex IV of FIR/01, showing the coverage of the relevant liabilities;

b) documentation of how the applicant has calculated the minimum amount in a way that is compliant with the referred Annex IV of FIR/01, including all applicable components of the formula specified there