ANNEX I: INFORMATION REQUIRED FROM APPLICANTS FOR AUTHORISATION AS PAYMENT INSTITUTIONS (PIs)

INTRODUCTION

This Annex supplements paragraph 34 of FIR/01. This Annex applies to applicants that intend to provide activity (a)-(g) of paragraph 2 of the Second Schedule to the Act or activity (h) of paragraph 2 in combination with other payment services. Applicants that intend to provide only activity (h) are subject to the specific set of guidelines for account information service providers (AISPs).

PROGRAMME OF OPERATIONS

The programme of operations to be provided by the applicant should contain the following information:

a) a step-by-step description of the type of payment services envisaged, including an explanation of how the activities and the operations that will be provided are identified by the applicant as fitting into any of the legal categories of payment services listed in the First Schedule to the Act.

b) a declaration of whether the applicant will at any point enter or not into possession of funds;

c) a description of the execution of the different payment services, detailing all parties involved, and including for each payment service provided:
   i. a diagram of flow of funds, unless the applicant intends to provide payment initiation services (PIS) only;
   ii. settlement arrangements, unless the applicant intends to provide PIS only;
   iii. draft contracts between all the parties involved in the provision of payment services including those with payment card schemes, if applicable;
   iv. processing times.

d) a copy of the draft framework contract;

e) the estimated number of different premises from which the applicant intends to provide the payment services, and/or carry out activities related to the provision of the payment services, if applicable;

f) a description of any ancillary services to the payment services, if applicable;

g) a declaration of whether or not the applicant intends to grant credit and, if so, within which limits;

h) a declaration of whether or not the applicant plans to provide payment services in other Member States or third countries after the granting of the licence;

i) an indication of whether or not the applicant intends, for the next three years, to provide or already provides other business activities as referred to in paragraph 3(a)-(d) of the

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

j) the information specified in a financial institutions rule on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance or other comparable guarantee under a financial institutions rule where the applicant intends to provide services (g) and (h) (PIS) and account information services (AIS)).

BUSINESS PLAN

The business plan to be provided by the applicant 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) where available for existing companies, certified annual accounts for the previous three years, or a summary of the financial situation for those companies 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;

d) information on own funds, including the amount and detailed breakdown of the composition of initial capital as set out in paragraph 31 of FIR/01;

e) information on, and calculation of, minimum own funds requirements in accordance with the method(s) referred to in FIR/02 as determined by the Authority, unless the applicant intends to provide PIS only, including:

    i. an annual projection of the breakdown of the own funds for three years according to the method used;
    ii. an annual projection of the own funds for three years according to the other methods.

GOVERNANCE ARRANGEMENTS AND INTERNAL CONTROL MECHANISMS

The Applicant should provide a description of the governance arrangement and the 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 payment institution'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.

MONITORING SECURITY INCIDENTS AND SECURITY RELATED CUSTOMER COMPLAINTS

The Applicant should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, 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 major incident reporting;

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

SENSITIVE PAYMENT DATA

The applicant should provide a description of the process in place to file, monitor, track and 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 payment institution'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) unless the applicant intends to provide PIS only, a description of how the collected data is filed;

f) unless the applicant intends to provide PIS only, 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

The applicant should provide a description of the business continuity arrangements consisting of the following information:

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) 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;

e) a description of the mitigation measures to be adopted by the applicant, in cases of the termination of its payment services, ensuring the execution of pending payment transactions and the termination of existing contracts.

COLLECTION OF STATISTICAL DATA

The applicant should provide a description of the principles and definitions applicable to the collection of the statistical data on performance, transactions and fraud consisting of the following

information:

a) the type of data that is collected, in relation to customers, type of payment service, channel, instrument, jurisdictions and currencies;

b) the scope of the collection, in terms of the activities and entities concerned, including branches and agents;

c) the means of collection;

d) the purpose of collection;

e) the frequency of collection;

f) supporting documents, such as a manual, that describe how the system works.

SECURITY POLICY DOCUMENT

The applicant should provide a security policy document containing 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, wallets, the payment engine, the risk and fraud management engine, and customer accounting;
   iii. the support IT systems used for the organisation and administration of the applicant, 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 applicant 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, and for all underlying payment instruments;

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.

INTERNAL CONTROL MECHANISMS TO COMPLY WITH AML/CFT OBLIGATIONS

Provide a description of the internal control mechanisms which the applicant will establish in order to comply with obligations in relation to money laundering and terrorist financing under the Prevention of Money Laundering Act and the Prevention of Money Laundering and Funding of Terrorism Regulations, consisting of:

a) the applicant's assessment of the money laundering and terrorist financing risks associated with its business, including the risks associated with the applicant's customer base, the products and services provided, the distribution channels used and the geographical areas of operation;

b) the measures the applicant has or will put in place to mitigate the risks and comply with applicable anti-money laundering and counter terrorist financing obligations, including the applicant's risk assessment process, the policies and procedures to comply with customer due diligence requirements, and the policies and procedures to detect and report suspicious transactions or activities;

c) the systems and controls the applicant has or will put in place to ensure that its branches and agents comply with applicable anti-money laundering and counter terrorist financing requirements, including in cases where the agent or branch is located in another Member State;

d) arrangements the applicant has or will put in place to ensure that staff and agents are appropriately trained in anti-money laundering and counter terrorist financing matters;

e) the identity of the person in charge of ensuring the applicant's compliance with anti-money

laundering and counter-terrorism obligations, and evidence that their anti-money laundering and counter-terrorism expertise is sufficient to enable them to fulfil this role effectively;

f) the systems and controls the applicant has or will put in place to ensure that its anti-money laundering and counter terrorist financing policies and procedures remain up to date, effective and relevant;

g) the systems and controls the applicant has or will put in place to ensure that the agents do not expose the applicant to increased money laundering and terrorist financing risk;

h) the anti-money laundering and counter terrorism manual for the staff of the applicant.

STRUCTURAL ORGANISATION

Provide a description of the structural organisation consisting of:

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 descriptions 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 relevant operational outsourcing arrangements consisting of:

   i. the identity and geographical location of the outsourcing service provider;
   ii. the identity of the persons within the payment institution that are responsible for each of the outsourced activities;
   iii. a clear description of the outsourced activities and their main characteristics;

d) a copy of draft outsourcing agreements;

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

   i. a mapping of the off-site and on-site checks that the applicant intends to perform, at least annually, on branches and agents and their frequency;
   ii. the IT systems, the processes and the infrastructure 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;
   iv. an indication of the national and/or international payment system that the applicant will access, if applicable;

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.

EVIDENCE OF INITIAL CAPITAL

For the evidence of initial capital to be provided by the applicant, the applicant should submit the following documents:

a) for existing companies, an audited account statement or public register certifying the amount of capital of the applicant;

b) for companies in the process of being incorporated, bank statement issued by a bank certifying that the funds are deposited in the applicant's bank account.

SAFEGUARDING ARRANGEMENTS

Provide a description of the measures taken for safeguarding payment service users' funds

Where the applicant safeguards the payment service users' funds through depositing funds in a separate account in a credit institution or through an investment in secure, liquid, low-risk assets, the description of the safeguarding measures should contain:

a) a description of the investment policy to ensure the assets chosen are liquid, secure and low risk, if applicable;

b) the number of persons that have access to the safeguarding account and their functions;

c) a description of the administration and reconciliation process to ensure that payment service users' funds are insulated in the interest of payment service users against the claims of other creditors of the payment institution, in particular in the event of insolvency;

d) a copy of the draft contract with the credit institution;

e) an explicit declaration by the payment institution of compliance with Article 10B of the Act and the Financial Institutions Act (Safeguarding of Funds) Regulations.

Where the applicant safeguards the funds of the payment service user through an insurance policy or comparable guarantee from an insurance company or a credit institution, the description of the safeguarding measures should contain the following:

a) a confirmation that the insurance policy or comparable guarantee from an insurance company or a credit institution is from an entity that is not part of the same group of firms as the applicant;

b) details of the reconciliation process in place to ensure that the insurance policy or comparable guarantee is sufficient to meet the applicant's safeguarding obligations at all times;

c) duration and renewal of the coverage;

d) a copy of the (draft) insurance agreement or the (draft) comparable guarantee.

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 on the criteria on how to stipulate the minimum monetary amount of the professional insurance or other comparable guarantee and Article 5 (1B) of the Act, the applicant for the provision of PIS or 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 therein.