The European Supervisory Authorities

Stockholm January 22, 2016

Response to Joint Consultation Paper JC/2015/61

1. Introduction

Klarna AB, corp. reg. no. 556737-0431, (”Klarna”) is a credit institution under the supervision of the Swedish FSA. The guidelines proposed by ESA will apply to our business. For this reason we would like to contribute by responding to this consultation.

We welcome the ESA guidelines and believe that they will raise the awareness on risk factors in the financial sector and increase the quality of firm’s AML/CTF efforts.

In addition to responding to ESA’s questions online, with this document we’d like to take the opportunity to comment on some sections and make a suggestion for another chapter with sectoral guidelines.

2. Our response to ESA’s questions for consultation (5.2)

a) Yes, but see feedback and suggestions below.
b) Yes, as far as we can tell from a supervised firm’s perspective.
c) Yes, it provides sufficient clarity on the scope.

3. General feedback

a) Impact assessment

Pages 83-87: We agree with ESA’s preferred options, with the following comments:

- <u>Consistency with international standards:</u> The regulatory landscape is split. For this reason we appreciate that ESA favors the option to provide an inclusive and all-encompassing document. If we should be efficient in combatting ML/TF, it is necessary to update these guidelines when new trends and modus emerge.

- Structure of Guidelines: We believe that there is a risk that less experienced firms do not find or consult both guidelines if ESA drafts two set of guidelines. Also, it is an advantage to see that the same factor may drive both higher and lower risk.
- Addressees: Firms often have activities in several sectors and for them it is easier to consult only one set of guidelines. In addition it is beneficial to all sectors that we can benchmark and be inspired by each other's risk factors. For these reasons we favor ESA's approach.
- Level of prescription: We agree with ESA that there is a risk that firms do not have sufficient awareness, expertise and sometimes willingness, to take on the larger responsibility that the less prescriptive approach impose on firms. However, we prefer that these guidelines are flexible since prescriptive rules tend to undermine efforts to create value-based compliance cultures in firms.

b) Non face-to-face situations

Comments to items 29, 30, 98, 104, 131 (i. customer's behavior), 133:

Remote customers and non-face-to-face situations are often presumed as facilitating anonymity and high risk /EDD. We would like to challenge this presumption and put it into perspective in regards to e-commerce. In e-commerce, the remote relationship is given. The convenience of shopping online is that you don't have to go anywhere. If you shop online, you expect to be able to choose payment method and make the settlement online too.

We agree with ESA that remote/online relationships can be considered as presumed higher risk where the customer can chose face-to-face contacts as an equally convenient alternative, or where competitors offer its equivalent services both face-to-face and online. However, if there is no element of avoidance of face-to-face contacts, it is incorrect to assume that online onboarding or transactions entail higher risk. We believe that identification of customers may be done just as reliably online due to electronic verification and other new technical solutions. Our identity is increasingly documented online rather than in physical documents. The increasing occurrence of fraudulent identity documents and impersonation fraud point to the weaknesses in face-to-face interactions. By tradition we still perceive face-to-face contacts as more reliable. We believe this is changing and should be reflected in the guidelines.

We suggest that ESA emphasizes "anonymity" and "avoidance" as the factors that drive higher risk - not the remote/ online interaction in itself.

c) Nature and purpose

Comments to items 10 (iii), 42 (ii), 57 (ii):

We believe that ESA should recognize the need for different approaches depending on the firms' business model when assessing the nature and purpose of business relationships and transactions. For some firms, like e-commerce payment facilitators, it should be recognized that a risk based approach allows such firms to make retroactive assessments of the nature and purpose provided that there is a highly standardized product or service. This means that the firm should be able to assume the nature and purpose. The benefit of this approach is that it is more efficient when firms may choose to put resources into defining and monitoring behavior that imply abuse or unintended use that deviate from such standardized nature and purpose of its products/services.

If ESA maintains that the nature and purpose of a certain product cannot be assumed, we suggest that ESA clarifies that knowing what is being financed is an example of establishing the nature and purpose of the transaction or relationship.

d) Factors of lower risk

Low risk transactions

Comment to item 99:

We suggest that ESA states that traceable payments is a factor that indicate lower risk. It should not be limited to payments that the firm can trace themselves internally, but also include payments that mandated authorities could trace. This distinguishes traceable payments from payments based e.g. on cryptocurrency, which normally cannot be traced or linked to an identified payer.

Disclosure requirements

Comment to item 101:

It would be useful if ESA could provide examples of good sources of information on companies that are under transparency /disclosure obligations that are sufficient.

e) Factors of higher risk

PEP

Comment to item 49 (senior management approval):

We would like to see a more risk based approach, which allows firms to determine on what level approval for entering into or continuing a business relationship with a PEP. To give an example, for us it would be inefficient if a senior manager must approve a PEP consumer who wish to part pay for an online purchase of clothes.

Tax havens

Comment to item 23:

It would be useful if ESA could provide examples of good sources of information on tax havens and jurisdictions with problematic (bank) secrecy rules.

f) Other

Good that ESA uses the terms "higher/lower" risk instead of "high/low" risk. This is less prescriptive and allows firms to have a nuanced approach, while making firms accountable.

4. Sectoral guidelines for "E-commerce payment facilitators"

The banking sector is undergoing a radical change. Large technical companies are entering the banking sector. Some experts believe that fintech soon will represent a bigger share of the banking sector than traditional banks.

Klarna is one of those larger European fintech firms, which provide payment solutions to e-commerce. The business models and market conditions are in many ways different for us and similar players. The business models are often a blend of regulated products and technical solutions. An example of our unique conditions, is that when we offer a payment method for an online purchase, we always know what the consumer is buying. Another example is that all our consumers are remote customers. This requires a shift in the traditional notion that face-to-face interaction is the standard, and remote interaction an exception.

In the proposal, the sectoral guidelines for retail banks, money remitters and for electronic money issuers are the guidelines that are the most relevant for our sector. However, our risks – and risk level - are not identical to those firms'. By default e-commerce payment facilitators are exposed to a lower risk since no cash is handled and payments are always made from/to regulated credit institutions. The payments sector has emerged due to a specialization in the transaction chain. The same result is achieved (the customer pays for a purchase) but more niched players are involved to make the transaction smoother. The firms can be both regulated and non-regulated. ML/CT risks do not increase in the transaction chain just because more firms participate. This becomes evident if you look at the transaction from the consumer's perspective. These conditions affects AML/CTF risk factors and the type of measures that are suitable to take by firms in this sector.

Our perception is that both national and EU rules are often drafted with large banks in mind. This makes it harder for other players to apply the rules and creates uncertainty. This may be a competitive disadvantage for such firms and make their AML/CTF work less efficient.

For these reasons, we suggest that the growing e-commerce payment sector is taken into account and is made visible when new rules are adopted. These guidelines are an excellent opportunity for ESA to show that fintech firms are on its mind. We have chosen to call this type of firms "e-commerce payment facilitators", but it could be made broader by using the terms "payment facilitators" or "payment firms".

Please find attached in <u>Appendix 1</u> a proposal for an additional chapter with sectoral guidelines.

You are welcome to contact the undersigned for any questions you may have.

Yours sincerely

Mikael Karlsson
Group Compliance Director

Phone: +46-70-0029166
Email: Mikael.karlsson@klarna.com

Appendix 1

Chapter X: Sectoral guidelines for e-commerce payment facilitators

This chapter provide guidelines for firms, which facilitate payments or products and services purchased online. Such e-commerce payment facilitators may be regulated as credit institutions, payment service providers or electronic money issuers. As this is a growing sector with some unique aspects, these sectoral guidelines are addressed to those firms. The sectoral guidelines for retail banks, money remitters and electronic money issuers may also be relevant.

Due to the nature of the products and services offered, the relative ease of access and the often large volume of transactions and business relationships, e-commerce payment facilitators are to some extent vulnerable to certain types of terrorist financing and mainly the layering and integration stages of the money laundering process.

The degree of ML/TF risks depends primarily on the features of the individual payment methods that the firms offer and what merchants are offered such payment methods.

Risk factors

<u>Product risk factors</u>

The following factors may indicate higher risk:
- The product's features might favor anonymity
- An unusually high volume or large value of transactions
- The product has a global reach
- The product can be used in cross-border transactions or in different jurisdictions
- The transaction is funded with anonymous electronic money (e.g. virtual currency or stored value cards)
- The product can be funded with payments from unexpected, unidentified or non-associated third parties, for example in the case of part payment products or revolving credits
- The product enables repayments to unknown accounts
- The product is designed to accept payments to merchants dealing in goods and services associated with increased financial crime risk
- The product allows person-to-person transfers

The following factors may indicate lower risk:
- The product has limited functionality (e.g. only available for payments to certain types of merchants, benefits can only be enjoyed by the customer)
- The product only allows transactions with merchants whose business is associated with lower financial crime risk
- The product only allows transactions within certain thresholds in value or number of payments

- The product requires that the funds for the transaction are drawn from an account/card held in the customer's name at an EEA credit or financial institution
- The product does not allow or enable overpayment
- The product can only be used domestically or in certain regions
- The product can only be used by a limited number of merchants whose business the firm is familiar with
- The product is designed to specifically restrict its use by merchants dealing in goods and services that are associated with increased financial crime risk
- The product is only accepted as means of payment for limited types of low risk services and products
- The product only allows payments to/from regulated financial institutions

Customer risk factors

The following factors may indicate higher risk:

- The customer is an undertaking associated with higher levels of ML/TF risk
- The customer is a PEP or an undertaking associated with a higher corruption risk
- The customer is a new undertaking without adequate business profile or track record
- The customer is a non-resident
- The customer's beneficial owners cannot easily be identified, for example because the customer's ownership structure is unusual or unduly complex
- The customer is reluctant to provide CDD information
- The customers transactions always stay just below any value/transaction limit
- The product appears to be used by several people whose identity is not known to the firm
- Frequent changes in customer's identification data, such as home address, IP-address, linked bank accounts
- The product is not used for the purpose it was designed for
- The customer's behavior or transaction volume is not in line with what is expected
- The customer's behavior is unusual

The following factors may indicate lower risk:

- The customer is a long-standing client whose previous transactions have not given rise to suspicion or concern
- The customer is a public company listed on a regulated market
- The customer is a domestic public administration or enterprise from a jurisdiction with low levels of corruption
- The customer is a credit or financial institution from a jurisdiction with an effective AML/CTF regime and is supervised for compliance with their AML/CFT obligations

Distribution channel risk factors

The following factors may indicate higher risk:

- Online and non-face to face distribution, without adequate safeguards
- Reliance on third party's CDD measures

- Intermediaries that do not have adequate AML/CTF systems and controls in place

Country or geographic risk factors

The following factors may indicate higher risk:
- The customer has significant personal or business links to high risk jurisdictions
- The product receives funds from sources in a high risk jurisdiction

The following factors may indicate lower risk:
- Countries associated with the transaction have an AML/CFT regime comparable to EU standards

Measures

Monitoring systems should be put in place. Examples include:
- Systems detecting anomalies or suspicious patterns of behavior
- Systems that identify discrepancies between submitted and detected information
- Systems that compare data submitted to data held on other business relationships
- Systems that identify whether the product is used with merchants dealing in goods and services that are associated with increased financial crime risk

Enhanced customer due diligence

Examples of EDD measures firms may apply in a high risk situation include:
- Verifying the customers and beneficial owners' identity on the basis of more than one reliable and independent source
- Obtaining more information about customer and the nature and purpose of the business relationship
- Obtain additional information during identification such as source of funds
- Increase frequency of transaction monitoring
- Review and update information and documentation more frequently
- Apply enhanced monitoring to the customer relationship and individual transactions

Simplified customer due diligence

Examples of SDD measures firms may apply in a low risk situation include:
- Update CDD information only in case of specific trigger events, such as the customer requesting a new or higher risk product
- Postponing the verification of the customer's or beneficial owner's identity to a certain later date after the establishment of the relationship or to when a certain threshold is exceeded
- Verifying the identity on the basis of fewer or less reliable sources
- Using alternative methods to verify identity

- Assuming the nature or intended purpose of the business relationship where this is obvious
- Reducing the intensity of monitoring as long as a certain monetary threshold is not reached

Klarna AB
Org nr: 556737-0431
Sveavägen 46
SE-111 34 Stockholm

Tel: +46 (0)8 - 120 120 00
Web: www.klarna.com
E-mail: info@klarna.com