Supervision expert centers
Trust and payment companies

Amsterdam
P.O. box 98
1000 AB Amsterdam

Date
24 March 2011
Your reference

Our reference
2011/179115
Handled by
Miro, A.
Direct dialling
020 524 1985
Enclosure(s)

Re:
Circular of De Nederlandsche Bank NV (DNB) for payment institutions providing money transfer services

1. INTRODUCTION

This circular is intended for (foreign) payments institutions providing money transfer services in the Netherlands. We request that you inform your agents and branches in the Netherlands of the contents of this letter.

The great risk entailed for a payment institution in providing money transfer services is that it becomes inadvertently involved in money-laundering or terrorist financing. The larger the number of transactions and the higher the number of different payors, the higher this risk becomes.

In 2010, to prevent abuse of money transfers by criminals, the Financial Expert Centre (FEC) launched a project entitled "Abuse of Money Transfers" to prevent abuse of money transfers by criminals.[1] Within the frame of this project the FEC partners have proposed a range of measures.

This letter brings **three important measures** to your notice, and provides you with guidelines to prevent your payment institution from becoming inadvertently involved in money laundering or terrorist financing. In its capacity of supervisor of payment institutions, DNB will pay special attention to these measures and their implementation inside the institutions' organisations. Arising from Sections 3 and 35 of the *Wet ter voorkoming van witwassen en financieren van terrorisme* or *Wwft* [Anti-Money Laundering and Anti-Terrorist Financing Act], these measures are designed to achieve:

1) adequate staff training;
2) effective transaction analyses;
3) enhanced data quality.

[1] The FEC is a multidisciplinary form of cooperation between seven partners, i.e. AFM (i.e. Netherlands Authority for the Financial Markets), the police authorities, Tax Authorities, the FIOD (i.e. Fiscal Information and Investigation Service), the Public Prosecutor's Office and the AIVD (i.e. General Intelligence and Security Service). The Ministry of Security and Justice and the Ministry of Finance participate in the FED as observers. More information about the FEC is available under www.fec-partners.nl

In Section 2, we will discuss the first objective, i.e. 'adequate staff training' and in Section 3, the objectives 'effective transaction analyses' and 'enhanced data quality'.

2 TRAINING

Under Section 35 *Wwft*, a payment institution must see to it that staff, to the extent relevant to the performance of their duties, are aware of the relevant provisions under the *Wwft* and receive the training they need to be able to detect unusual transactions.

DNB also holds that the number of unusual transactions detected will increase if staff is adequately trained. Payment institutions are therefore required to observe the following **guidelines**:

1. For every individual employee, the institution formulates a **tailor-made training plan**. This plan should cover the data on training courses followed or yet to be followed (When were they attended? What were the results?)
2. Before commencing his/her job, each newly appointed employee will need to have completed all training courses considered necessary for the proper performance of his/her duties. This is laid down in the training plan.
3. Employees must not only be made, but also remain, aware of the provisions under the *Wwft*. To this end, periodical **refresher courses** are required. The schedule and completion of these refresher courses are also laid down in the training plan.
4. The payment institution (internal control) **conducts periodical checks** for compliance with the above conditions.

DNB is of the opinion that, by observing the above guidelines, an institution will operate in compliance with Section 35 of the *Wwft*. However, following the guidelines alone is not enough. In addition, the institution will also be required to demonstrate that it operates in the spirit of the guidelines. For example, by giving cashiers feedback on the basis of the outcomes of internal controls, since this too can help improve employees' knowledge. To be able to so adequately, the outcomes of internal controls must be properly recorded.

3 TRANSACTION ANALYSES

Under Section 3 *Wwft* an institution is required to subject clients to a **customer due diligence review** within the scope of the prevention of money laundering and terrorist financing. This procedure is conducive to better monitoring of financial transaction flows and quicker detection of unusual transactions.

DNB is of the opinion that the transaction analyses as performed by a number of payment institutions are too limited. From a random check performed by DNB, it emerged that a considerable percentage of the transactions (20 to 45 percent, depending on the agents and branches location) occur within networks that should be subjected to supplementary investigations. Often these transactions are mistakenly marked 'not unusual'. As a consequence, a payment institution may:

- pass on incomplete (subjective) information to the FIU-NL;
- approve transactions that should have been rejected, at the risk of becoming involved in money laundering;
- consider a thorough customer due diligence review ('Know your customer') unnecessary.

DNB expects payment institutions to perform periodical analyses in order to gain more insight into unusual transactions. If they do so, they will be better equipped to take suitable measures. DNB is of the opinion that a payment institution should at least perform the analyses referred to in the following section.

3.1 Standard transaction analyses

During its supervisory visits, DNB will discuss the outcomes of the transaction analyses performed by the payment institutions, paying particular attention to the following points:

Send transactions
- selection on the basis of the sender from the Netherlands;
- selection on the basis of the receiver abroad.

Receive transactions
- selection on the basis of the receiver in the Netherlands;
- selection on the basis of the sender abroad.

When are you ordered to conduct the transaction?
- On a monthly basis: last month's transactions.
- On a quarterly basis: last quarter's transactions.
- On an annual basis: last year's transactions.

These selections of send and receive transactions may help you in your investigation into suspicious money transfers. For small institutions, a top 10 per category usually suffices, for large offices a top 50 is preferable. It is left to the institution's **own responsibility** to decide on the size of the selection.

DNB considers it useful that an overview is obtained of the main (large) Dutch and foreign clients and that these clients are subjected to a customer due diligence review. An institution must verify if it has sufficient information about the origin and destination of money. If it has not, or has doubts about the reliability of the information, an institution must take suitable measures. Think, for example, of instructing cashiers to inquire after the origin and destination of the money the next time the customer visits the bank. The cashier may ask the customer to present substantiating documents, like an extract of the Chamber of Commerce or an invoice.
If a sender or receiver sends or receives large amounts from abroad, the investigation will usually focus on the Dutch customers who conduct business with this person. This course is often followed as in most cases payment institutions in the Netherlands cannot obtain background information on senders and receivers in other countries.

DNB considers all of the abovementioned measures as the **minimum level.** DNB expects that a payment institution, depending on the number of transactions and the sort of risk involved, conducts a supplementary investigation. A supplementary investigation might cover:

- specific regions or countries (corridor investigations);
- the addresses of Dutch clients involved in the transactions (verifying if the addresses are no fake addresses and if they are not used for other individuals as well);
- transactions just below the objective reporting limit ("smurfing");
- analyses per location;
- the ratio between send and receive transactions;
- transactions within the Netherlands or Europe;
- reports of unusual transactions;
- network analyses. **Network analysis tool,** which may have added value for medium-sized and large payment institutions. By means of these applications, transaction networks can easily be traced and charted to reveal any abuse made.

As DNB will discuss the outcomes of these analyses with the institution, it expects that the institutions record their transaction analyses and are able to make this documentation available to DNB, if so requested.

If the outcomes of transaction analyses should reveal a high incidence of unusual transactions, you are advised to contact your contact at FIU-NL in order to discuss how you should notify these transactions.

3.2 Data quality

To be able to monitor and analyse transactions effectively, the (source)data must be correct and up to date. To guarantee that this is the case, customer and transaction data entries must be **accurate, complete** and be **uniform in format**. DNB therefore expect institutions to enter the identity documents of clients accurately, and make sure that the data are complete and accurate. DNB also expects payment institutions to be alert to the quality of their source data and aware of the improvements still required to enable effective transaction analyses.
By observing the following guidelines, you will improve the quality of the data:

- Country code: use **ISO country codes** (ISO 3166-1-alpha-2 see: *http://www.iso.org/iso/english_country_names_and_code_elements*).
- Address of client: ask the client for his/her **postal code** and enter this in *http://www.postcode.nl/* to copy and paste the corresponding street name.
- Name of client: enter the **family name** in **capitals** and the **given name(s)** in **small letters**. This ensures that in transaction analyses the family name and the given name(s) can be easily distinguished from each other.
- **Transaction date**: when entering a send and receive date, we would advise you to use the following format: **dd-mm-yyyy**. For example: 01-03-2011.

4 IN CONCLUSION

Within the scope of the fight against money laundering, DNB considers it vital that financial transfer flows within the money transfer market be closely monitored. For this reason, DNB will shortly start to analyse the transaction data of that market. In the short term, you will receive a letter requesting you to report the **transaction data on the first quarter of 2011** to DNB.

Should you have questions further to the above, please contact Mr F.W. Sonneville at the telephone number stated in the header of this letter.

Yours Sincerely,
De Nederlandsche Bank NV

Ms Heidi A.A. Broekhuis
Head of Department

Arthur Sonneville RA
Examining Officer