DeNederlandscheBank
EUROSYSTEEM

National Institutions
Supervision Division
Payment Institutions and
Special Projects Department

Presentation by Hendrik Jan Boehlé at the seminar for payment institutions "Seven tips for ensuring that your institution is compliant" of Wednesday, 9 September 2015[1]

[1] Should you have any questions, please contact Hendrik Jan Boehlé at H.J.Boehle@dnb.nl;

Disclaimer:

- This is the unofficial English translation of the literal transcript of the introduction by the Head of the Payment Institutions and Special Projects Department at the seminar for payment institutions "Seven tips for ensuring that your institution is compliant" of Wednesday, 9 September 2015, at the premises of De Nederlandsche Bank in Amsterdam. This text may not represent a one-on-one rendering of what was said during the introduction.
- No rights may be derived from this presentation.
- The official legal text as published in the Government Gazette prevails at any time.

Slide 2: "Contents"

- My main objective in holding this presentation is to give you an idea of what prudential supervision means for your institution.
- In the next twenty-five minutes, I will be explaining to you what prudential supervision means and, above all, how it affects you. And perhaps even how you can avoid being affected. Right at the end, during the last five minutes, I will be available for any questions you might have. Any questions that we don't get around to dealing with, I will be happy to discuss in one of the breaks or over drinks.
- First let me show you how we have organised our supervision of payment institutions at DNB. I will then mention a few areas of emphasis in prudential supervision and two thematic examinations, which will give you a concrete picture of what we have been up to in your sector as a supervisory authority, and why we do what we do.

Slide 3: "How have we organised supervision at DNB?"

- We currently have sixteen divisions.
- There are various divisions that might contact you, asking for information or proposing a meeting. In practice you will most likely be contacted by our Payments Division, our Statistics Division, our National Institutions Supervision Division or our Horizontal Functions and Integrity Supervision Division.
- Within our National Institutions Supervision Division, our Payment Institutions and Special Projects Department is responsible for supervising payment institutions.
- And within our Horizontal Functions and Integrity Supervision Division, our Thematic Supervision of Integrity and Expert Centre for Integrity Strategy deal with integrity supervision.
- However, you may also get to deal with other departments within the context of supervision of payment institutions. In practice, they will be, within our Horizontal Functions and Integrity Supervision Division, our Expert Centre Market Access, our Expert Centre Fit and Proper Testing (which screens decision makers and co-decision makers) and our Expert Centre Intervention and Enforcement.

Slide 4: "How have we organised supervision at DNB?"

- [This slide shows you the names of the individuals you may get to know. They supervise payment institutions.]

Slide 5: "Who do we supervise?"

- Since the European Payment Service Directive I (or PSD1) entered into effect on 1 September 2009, we have supervised around forty payment institutions.
- Prudential supervision of payment institutions is carried out by our Payment Institutions and Special Projects Department, which is part of the National Institutions Supervision Division.
- Within the Horizontal Functions and Integrity Supervision Division, our Thematic Supervision of Integrity Department is responsible for integrity supervision of payment institutions and account supervision of money transfer institutions.

Slide 6: "How do we supervise?"

- We follow a supervisory approach named FOCUS! to monitor financial stability and ethical operational management in the financial sector and by financial institutions in the Netherlands.
- FOCUS! represents a risk-based approach to supervision. [More detailed information about FOCUS! can be found here: http://www.toezicht.dnb.nl/en/binaries/51-225814.pdf]
- We use a very broad definition of risks that goes beyond financial risks. We also look at credit risks, operational risks, reputation risks, legal risks, ICT risks and outsourcing risks. They must all be addressed, if only in the consumer's interests.
- The institutions we supervise come under a supervisory category. Those in supervisory category T3 have dedicated account supervisors, while those in T2 are subject to group supervision.

Slide 7: "How do we supervise?"

- We use a range of instruments to conduct our supervision. Those that we use most are reporting, regular contacts, acting on signals and thematic examinations.
- Our first instrument is reporting. Institutions submit various reports to us:
  - Prudential financial reports, twice a year

  - Approved annual report, the external auditor's audit report and management letter (before the end of June each year
  - Integrity report (once each year)
  - Monetary reports (various reports, such as with respect to payment services and to the ECB)
- Our second instrument is regular contacts.
  - Institutions in supervisory category T3 have dedicated account supervisors, with whom they are in touch on a regular basis.
- The third instrument we have is that we act on signals we receive. Examples include information provided by (inter)national supervisory authorities or the media, complaints and reports from whistle blowers.
- The fourth instrument are the thematic examinations we conduct. This year's examinations focus on three themes, which are quality of reporting, systematic integrity risk analysis, and safeguarding of customer accounts and compliance with the strict separation of assets under Section 3:29a of the Financial Supervision Act to protect consumers' funds.

Slide 8: "What are our greatest concerns in ongoing supervision of payment institutions?"

- Prudential supervision focuses on the financial solidity of payment institutions, which is their resilience in dealing with losses or reduced income.
- Sound and ethical operational management should safeguard such financial solidity.
- We use a wide definition of sound operational management. My colleague Juliëtte van Doorn will deal with ethical operational management in more detail.
- There are a number of topical items on which we place additional emphasis in our ongoing supervision. This means they may be the subjects when you are in touch with one of our supervisors. They are:
  - governance;
  - safeguarding customer accounts, which means protecting consumer funds;
  - solvency;
  - operational risk, including cyber threats;
  - data quality; and
  - business models.

Subject Governance

- We believe good and effective governance is of fundamental importance.
- The concept of governance refers to your institution's management set-up:
  - its structures;
  - its division of duties and powers;
  - its strategy;
  - its policy and processes;
  - its internal control functions;
  - the method and depth of rendering account of the policy pursued; and
  - the expertise, competences, experience, availability and suitability of the members of your Executive Team, Management Team or Board of Management and of the members of your Supervisory Board.
- Good governance in financial institutions is a precondition for sound operational management. It should ensure that you risks identify in good time and control them and that you render account of and communicate about your actions, internally and externally, in a transparent manner.
- Adequate checks and balances within an enterprise strengthen risk management and minimise the likelihood of problems occurring.
- This is why in our supervision we devote a great deal of attention to:
  - the manner in which your institution is organised;
  - the division of responsibilities and powers in your institution and in your Executive Team, Management Team or Board of Management;
  - the extent to which your compliance officer, risk manager and internal audit alert your Executive Team, Management Team or Board of Management, as well as your Supervisory Board, to risks, both invited and uninvited,
  - the effectiveness of your institution's three-lines-of-defence model;
  - the quality of the reports and the reporting systems used to render account of the policies pursued; and finally
  - whether ICT systems actually enforce segregation of duties.

Slide 9: "Theme: Safeguarding customer accounts"

- One example of our prudential thematic examination is our examination of the safeguarding of customer accounts and compliance with the strict assets separation under Section 3:29a of the Financial Supervision Act to protect consumer funds.
- Let me just walk you through this, because it will give you a good picture of how you may get to deal with us, how it works and, most importantly, why this is so important.
- Our underlying rationale is that protecting consumer funds is crucially important, because the consumers' confidence in payments and payment institutions may not be harmed. The unlawful use of consumer funds is a mortal sin, which is why we believe high standards should govern your institution's management of customer accounts.
- Back in April, we asked all payment institutions to complete a questionnaire, except those holding an authorisation for service number six, which is money transfers. We requested information on asset separation, more particularly about risks, set-up and practical details in terms of operational management. In asking these questions, we mainly aimed to gain insight into the instruments used, such as a customer accounts foundation, bank guarantees or insurance policies.
- In the second phase of our examination, we selected a number of payment institutions for on-site inspection.
- Just to give you a few notable issues:
    - Strict asset separation is clearly below par at a number of institutions. This means that institutions should take measures to improve this, or provide guarantees or insurance cover to better protect customer ownership rights. Some legal entities are too closely interwoven with the authorised entity or other legal entities.
    - Some customer accounts foundations insufficiently safeguard the protection of customers' ownership rights.
    - In those cases, stricter control requirements should apply, including audits performed by external auditors.
    - Rights and obligations are not always formally documented in management agreements. Examples of formal arrangements that we found lacking are:
        - a description of the nature and scope of the services;
        - arrangements on the fees charged by the payment institution for the services provided to the customer accounts foundation;
        - arrangements on the withholding of commission and other fees and charges;

    - rights and obligations of legal entities, such as the payment institution and the customer accounts foundations; and
    - authorisations.
  - Practice shows that clearing & settlement and reconciliation of transactions still involves a great deal of manual sorting out and unexplained differences. Only a small number of institutions appeared capable of performing timely reconciliations.
- Put briefly, in our opinion, additional requirements governing the set-up must be drawn up to ensure better safeguarding of customer accounts. To formalise those requirements, we are currently drafting Q&As or possibly a Policy Rule to prescribe improvements in set-up.
- We will submit a Policy Rule to your and other relevant stakeholders for consultation. We aim to publish the Q&As or a Policy Rule by the end of this year. Of course, you remain responsible for taking prompt action to fully safeguard the safety of consumer funds. Please use the tips I gave you to your advantage.

Subject Data quality

- Reports are an important source of information for us, and we use them in our supervision on a daily basis. That's why we've looked into the quality of the prudential reports,
- This has led to some changes in the reporting formats. Due to time constraints, I will limit myself to mentioning the two new reports we introduced. They are more closely in line with FINREP and COREP reports, which we already apply in our supervision of banks and investment firms.
- It has proved quite a challenge to design a fixed reporting template for a diverse category of institutions. So we decided to use the new format after consulting with three payment institutions.
- You can of course ask us for help with specific line items.
- We still have some way to go, but the new format is a big step in the right direction.
- Incidentally, we will be paying closer attention to the quality and timeliness of the financial reports that payment institutions submit, in the interest of an effectively functioning system. We already do so for other supervised institutions.

Subject Capital Requirement

- One of the authorisation requirements for payment institutions is that they must at all times have the minimum solvency capital, calculated on the basis of

method A, B or C pursuant to Section 60a(1) of the Decree on Prudential Rules for Financial Undertakings.

- Financial institutions must be in good financial health if they are to be trusted by other economic operators.
- We expect you to meet the minimum solvency requirement at all times
- We also expect you to have insight into threats to your solvency capital at all times, to that you can take timely and adequate action where needed.
- The minimum solvency capital is an ongoing requirement. Especially when using "method B" for calculating the requirement, growth in transaction volumes will cause the required minimum to increase sharply. Please be aware of this.

Subject Business Models

- This is a relatively new area in our supervision, and it is mainly forward-looking, dealing with the sustainability of financial institutions.
- This means we analyse in great detail at how an institution generates its income. This requires that we peel the onion as it were, layer by layer, delving into an institution's key sources of profit and its vulnerabilities.
- Monoliners, in particular, may be vulnerable to changes in market demand.
- As regards overall profitability of payment institutions, we receive an increasing amount of signals about strong pressure on prices and profit margins.
- Our expectation is that this pressure may continue to increase, given the rising number of market players in the Netherlands and the modified fee structures of Visa and MasterCard, forced by the European Commission.
- While such pressure may benefit competition and innovation in the sector, the resulting price erosion and shrinking profit margins give cause for concern. After all, you need profit margins to pay the cost of complying with statutory requirements.
- Price erosion may carry the risk of institutions lowering guarantees in their safeguards to be permanent compliant with legal requirements. They may do so, for example, to:
  - reduce compliance costs;
  - gain a competitive edge by accepting customers without due care or being less critical of a merchant's activities; or
  - failing to raise the quality of risk management, compliance and internal audit in line with the increase in numbers and risk profiles of customers and payment volumes or with the institution's own growth.
- We will not accept this and take enforcement measures where needed. We will not allow the consumer's confidence in the payment system to be eroded

because certain parties choose not to comply with statutory requirements as set out in the Financial Supervision Act, the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act. Every payment institution is obliged to comply with those requirements, and compliance inevitably costs time and money.

- That sounds harsh, and it is. As National Institutions Supervision Division Director mentioned in his introduction to the seminar, our supervision is our legal task, but we execute it because we believe in it from the bottom of our hearts. The law is here become society demands that payments and everything connected with them are safe. And we are here to see to it that your sector also adheres to the law. If you have any questions about compliance or wonder how you could comply with specific provisions, keep checking our website and our Open Book on Supervision pages, but also speak your mind, here, today.

Slide 10: "Cyber threats"

Subject Operational risk

- Internationally, operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This definition also encompasses legal risk.
- Operational risk of course entails more than the example of cyber threats mentioned on this slide, but the importance of preventing cyber crime simply cannot be overrated.
- Recent examples of cyber attacks have shown that we must constantly be on the look-out for cyber crime, which is not something remotely relevant, but a real danger.
- Just to cite two of those examples:
    i. the DDoS attacks on several of your institutions back in May made by a criminal group that is still active internationally; and
    ii. the recent DDoS attacks on several nationally operating companies and agencies.
- As regards cyber threats, the big question is "when is it my turn?"
- Cyber threats are not merely an ICT issue, nor do they concern your ICT director alone.
- As payment institutions, you should be on the look-out, because you manage large sums of money. Those sums of money on the bank accounts of your customer accounts foundations make you an interesting target for those with bad intentions,

- who could be inside your institution, such as staff members having fingers in the till, but also outside. For example, an unauthorised person might gain access to your systems,
- which could cause large financial losses and might even jeopardise the continuity of your payment institution's services. Even more dramatic damage can be done if customers lose their trust in the payment system as a whole.
- There appears to be anecdotal evidence suggesting that cyber criminals also target in-house accounting systems, which seem to be the weakest links in the payment chains. Both external and internal systems must be adequately secured.
- Securing in-house systems may demand other precautionary measures, such as:[2]
  - using malware detection and anti-virus systems, with a particular focus on weaker links and programmes operating on a network; and
  - performing controls designed to detect manipulation of payment orders that transfer funds from a bank account to the bank account of a "money mule" rather than of a customer.
- Naturally, such precautionary measures cost money, time and effort, but as the adage in the aviation industry goes: "if you think safety is expensive, try an accident unsafety which is far more expensive".
- [Your payment institution should be prepared for serious situations. How well is your crisis management prepared for cyber threats? What does your communication strategy look like in the event of cyber threats?]
- In the area of dealing with cyber threats, the main responsibility lies with you. You can mitigate the risk of cyber threats by having audits performed from time to time or perform regular penetration tests.
- In addition, it might be a good idea if closer sector collaboration emerged, so that you keep your sector safe together. As a supervisory authority, we would be happy to assist.
- Working together by sharing ICT safety information. Other sectors have established platforms referred to as Information Sharing Analysis Centres (ISACs).
- Collaboration in the area of safety with other parties, such as banks and ICT service providers would also be a good idea.

[2] A further example is training your staff to raise their awareness of cyber risks and mitigate the risk of manipulation. You should also foster a culture of openness to reports, so that staff members are encouraged to report suspicious circumstances. We should all realise that anyone could be fooled into a cyber criminal's tricks and that no-one ought to be ashamed after it has happened. Feelings of shame and fear of negative reactions should never stop someone from reporting an incident. After all, it is crucial that intrusion risks are promptly reported, so that potential damage can be kept to a minimum.

- Finally, if your institution falls victim to attempted or actual cyber crime, please **notify** us. Your reports can help us identify the risks to which the sector is exposed and initiate joint action where needed and possible, so that we can prevent cyber crime from causing further damage.

Slide 11: "What can you expect from our prudential supervision in the next few months?"

- Looking at the next few months, we will be issuing more detailed guidance in several areas related to the Financial Supervision Act. More specifically, we expect to provide further guidance on customer accounts management in late 2015.
- The way things look now, our thematic examination in 2016 will address business models, but we may also look into the other aspects I mentioned before.
- What else can you expect of us in the period ahead? We will be devoting more energy to keeping in touch with you.

Slide 12: "Communication with and from DNB?"

- We will be sharing information with you in various ways.
- First, there is Open Book on Supervision. Go to http://www.toezicht.dnb.nl/en/index.jsp. Then, under "Sector", select "Payment Institutions".
- Secondly, we publish our English Payment Institutions Newsletter every three months. It includes practical information, e.g. on examinations about to be launched or recently completed, and announcements on legislative changes or the implications of new policies. Please verify whether the members of your Board of Management and Supervisory Board have subscribed to the newsletter and make sure they register where applicable. They can do so at http://www.dnb.nl/en/news/news-service/subscribe.jsp. You can also use this link to subscribe to our other English publications, such as Open Book on Supervision updates, which will keep you informed of developments relevant to your institution at regular intervals and without delay.
- Thirdly, we communicate by secure email. We aim to always exchange company-sensitive information with supervised institutions by secure email. The reason for doing this is that unsecured email traffic does not provide sufficient guarantees that information can be exchanged without unauthorised third-party access. We are currently setting up secure email connections

between us and yourselves. Please check the progress made thus far in realising your secure email connection with DNB.

- The Payment Institutions Newsletter of July 2015 provides some examples with respect to notifying us of significant events and incidents (http://www.dnb.nl/en/news/dnb-nieuwsbrieven/nieuwsbrief-betaalinstellingen/nieuwsbrief-betaalinstellingen-juni-2015/dnb323408.jsp)
- Of course, it is also up to you to gauge whether a significant event warrants a notification to DNB. The Financial Supervision Act sets open standards, which are often detailed in guidance documents prepared in consultation with experts and sector representatives. But even guidance documents do not lay down everything down to the last detail.
- Making a notification may be a nuisance, but failing to make it may turn out to be a much bigger nuisance if we find out.

Slide 13: "Tip 3"

- Before ending my presentation, I would like to give you the third of the seven tips of this afternoon. Although I had offered multiple suggestions, I was asked to restrict myself to revealing just one tip. So here's my tip: Never hesitate, but notify us immediately. "Be sure to notify us promptly in case of significant events or incidents." It's always better to make too many notifications than too few ("better safe than sorry"). And it's better to make them sooner than later.

- Thank you very much for your attention.

Slide 14: "Questions?"