Steven Maijoor: Paying attention – on the supervision of payment institutions

Speech by Mr Steven Maijoor, Executive Director of Supervision of the Netherlands Bank, at the Netherlands Bank Seminar "Supervision of Payment Institutions", Amsterdam, 14 April 2023.

* * *

Hello everyone.

Out of curiosity and because I knew I would be talking to you today, I checked my banking app to see how many times I recently used one of your services.

And even though I work for De Nederlandsche Bank, even though I am a supervisor and I know your sector well, I was still amazed at how often I saw one of your names appear.

I saw one of you when I bought some sailing gear.

I saw one of you when I ordered tickets for the St. Matthew Passion.

And I saw one of you when I donated to a charity.

There are already 81 licenced payment institutions in the Netherlands. And all 81 of you help businesses thrive. All 81 of you help people, like me.

Online, when we scroll, select and then securely pay. Or offline, when we pay at one of your pin terminals or with a QR code. Or when we check our bank account, after everything is paid for, to get an insight into our spending patterns.

All this means you have become a cornerstone of our financial system. And all this means you have become part of the financial supervision of De Nederlandsche Bank.

Formally, our supervision of your industry is rooted in the Payment Services Directive from 2009, PSD1, and the update, PSD2, from 2019. It is also rooted in the Anti-Money Laundering and Anti-Terrorist Financing Act from 2008.

Theoretically, one could say that supervising the trustworthiness of our financial system is about finding the right balance between entrepreneurial opportunities and stability risks.

Practically, supervision has to do with mapping, measuring and monitoring the risks to which you, and with you the entire financial system, are exposed.

Let me illustrate this – with a credit risk example, and a cyber risk example, but first with an example related to integrity risk.

An estimated 16 billion euros a year – that is how much criminal money is earned in the Netherlands. Half of this amount finds its way abroad. And from abroad, another 5 billion will find its way back to the Netherlands.

Often that dirty money is looking for a way to get clean. And when it does, it's not a good thing. Because it undermines trust – trust in our rule of law, in the security of our society, and in the integrity of our financial system.

In addition to banks, more and more people and businesses are relying on you for payment transactions. And it's your job – at least in part – to accept only clean money. To refuse dirty money. To guard the gate to the financial system, and in doing so, to keep it clean. Or at least, clean-ER.

Of course, there are many gates to the financial system – and you only have to guard yours. But criminal money will try every gate – so we depend on each other to keep the system we work in, the system we work on, to keep that system as clean as possible.

Next to this type of integrity risk, another type of integrity risk has received a lot of attention recently. And that is sanction risk.

After Russia invaded Ukraine, an act of aggression that is, by any measure, unjustified – the European Commission introduced a whole package of sanctions. And those sanctions are partly designed to prevent certain transactions to and from Russians on the sanctions list.

And also in this case, you have a vital role to play.

At De Nederlandsche Bank, we are very aware of the investments your industry has already made to guard your gate. Regarding anti-money laundering. Regarding anti-terrorist financing. And regarding sanction risk.

But unfortunately, we also know that some in your sector are still lagging behind. That in too many cases, basic housekeeping to mitigate these important risks is still insufficiently organised. To those of you to whom this applies, I say: we expect more from you.

And let me add that you can also expect something from us, your supervisor. And that is our commitment to focus our supervision on where risks can actually materialise. And that we can have a conversation about this.

Let me illustrate this.

Your sector raised a concern to DNB regarding the obligation to screen all transactions from all shoppers. While I do not want to go into legal and technical details, I do want to emphasize that we take your feedback seriously.

Of course, I understand that when I buy a book on sailing online, and my payment goes through one of your institutions, it has little value added for us if we require you to check whether or not I am on the sanction list.

When you see that I have a Dutch banking account, it is highly likely that I was already screened against Dutch sanctions lists by my issuer institution. And when I am buying something from an online bookstore, I am very likely paying for a book. So, in this case, what actual sanction risk would there be, right?

Well, you know just as much as I, that, in reality, things are often not that straightforward.

Suppose you are less convinced that I am buying a book. Suppose I could be buying image intensifier tubes, a so-called dual use good. And suppose I do not use a Dutch banking account to pay for it, but a foreign one.

Supposing all that, could the benefit of screening on your end get the upper hand?

I am merely asking the question. I don't have an answer.

But what I do have, is three things you can expect from us.

Going forward, we will bring your concerns to the attention of the Ministry of Finance and share insights from our supervision. This ensures that your concerns are taken into account in the upcoming update of the sanction regulation.

We will also discuss this at the European level – to improve the level playing field in Europe.

Third, and at this moment probably most important for you, we are aware of the fact that institutions do not screen each domestic shopper payment. But in the meantime, we won't spend scarce supervisory resources on this. We have other priorities.

But I will, of course, insist that you know where your higher risks lie, and that you mitigate these accordingly. And in that respect, there is still enough work to do for the sector, for example when it comes to improving the detection of transactions related to dual use goods.

Let me now turn to my second example. This has to do with cyber risks – a kind of risk that, over the past years, has increased significantly, and with the war in Ukraine even further.

Also for you.

We know that in the past some of you have already had to actively – and successfully – defend your institution from cyber threats.

It is, of course, no wonder that cyber threats are on the rise.

Looking at the broader financial sector, we have seen that, over the years, financial institutions have been morphing more and more into IT companies with a financial licence. More and more of what financial institutions do, takes place digitally. As a consequence, the IT infrastructure has become more and more essential to the functioning of financial institutions as a whole.

Looking at the payments industry, you are the prime example of this broader evolution. And your digital infrastructure forms the very core of your operations.

It is no wonder then, that you are well aware of cyber threats, and as a consequence, that you have robust defences in place against attacks like DDoS.

But cyber threats are growing in number and variety – so we must remain vigilant. That is why I am worried about what we found in our sectoral review of IT risks. We found that payment institutions still only make limited use of existing cyber security frameworks. Or of sectoral security intelligence and information sharing groups such as ISAC and CERT. Because even though there is a dedicated ISAC for payment institutions, we found that most of you are not participating in it.

Why is that?

From our experience with other sectors, we know that external resources, such as information sharing groups, can be beneficial. We know that by exchanging cyber intelligence amongst peers, you can increase your cyber resilience. So why doesn't this happen more?

My aim as supervisor is to safeguard trust in the financial system – a system of which you are a cornerstone. And that is why cyber threats, no matter how they appear, are high on my agenda – and that is also why they should remain high on yours.

My third and final example has to do with credit risk.

On March 10th, Silicon Valley Bank went bankrupt – as you all know.

Silicon Valley Bank was one of the go-to banks for fintech businesses on the other side of the Atlantic. If you were not mainly operating here on our side of the Atlantic, you might have worked with Silicon Valley Bank – for instance to deposit your clients' funds.

But also on our side of the Atlantic, payment institutions use third parties to deposit their clients' funds for safekeeping.

And here lies a risk, or at least a responsibility. The responsibility to monitor the creditworthiness of that third party.

Unfortunately, we know from our thematic examination on safeguarding that a number of payment institutions do so insufficiently. What's more – when drafting risk analyses, some payment institutions pay too little attention to the operational and financial risks of the third parties they rely on.

It goes without saying that what happened to Silicon Valley Bank was the result of poor risk management. And what happened, seriously damaged trust in the financial system. You don't want that. And we don't want that. So that is why an important part of our supervision focuses on the way you work with third parties. On the way you monitor and mitigate the risks that come with working with third parties – be it a cloud service

provider or an IT vendor. But our supervision also focuses on the way you manage financial exposures. And certainly on how you select banks to deposit your customers' funds.

When I looked at my bank statements, I was amazed by how much I rely on you, payment institutions.

And along with me, many others in the Netherlands do so too.

The thriving payments industry in our country is reflected in the enthusiastic use of your services by tons of Dutch businesses and organisations.

You can be proud of that – of being at the forefront of our digital society.

But with that success comes great responsibility. People rely on your services. Businesses depend on you. But many risks – and I only touched on integrity risks, cyber risks and credit risks – but many risks loom around the corner.

In order for people and businesses to continue to rely on you, those risks need to be dealt with. They need to be mapped and measured, monitored and mitigated. And they definitely need to be a topic of conversation.

That is why I am grateful to see so many of you here today. So that we can share stories and worries. Questions and concerns. Expectations met- and expectations unmet.

In short, the better we understand each other, the better we can keep our financial system as clean and secure as possible.

I wish you all a frank and fruitful afternoon.

Thank you.