**Thomas Egner**
**Secretary General, Euro Banking Association**

**Keynote remarks, Payments Risk Symposium**
**TCH and bpi, 2019 Annual Conference**

**19 November 2019**

**Check against delivery**

Thank you very much, James, for your kind introduction.

Ladies and Gentlemen, dear Colleagues, dear Friends,

It is a great honour and a great pleasure for me to contribute a few keynote remarks to this Payments System Risk Symposium.

If we look back on the last three decades of payment system risk management, it is relatively easy to identify specific risk trends for each of these decades.

In the years preceding the turn of the century, risks related to major changeovers were on everybody's mind. I am sure, quite a few of us here in the room still recall the doomsday scenarios that were part of many risk assessments of the Y2K bug. And if you have ever taken a look at the comprehensive plans we Europeans designed for the introduction of the euro in 1999 and in 2002, you might have thought we were making plans for the end of the world.

This is not surprising. Because we actually were making plans for the end of the world - for the end of the world as we knew it. But let me park that thought for the moment, so we can move forward in time.

Post 9/11, the first decade of the 21st century was marked by a strong focus on operational risk and business continuity considerations. The magnitude of the 9/11 terror attack prompted payment system operators across the world to implement, among other things, contingency perimeters geared at withstanding situations with one or two operations sites affected by the same calamity. And quite a few of these perimeters may have been reviewed and further expanded after a tsunami, triggered

by an earthquake in the Indian Ocean, struck over a dozen countries towards the end of 2004, killing an estimated 230,000 people.

Towards the end of that decade, financial risks, such as credit risk and liquidity risk, became the new centre of attention in the aftermath of the financial crisis that had hit the world in 2007-2008: while payment systems around the world had been beacons of stability during the crisis, new standards, such as the Principles for Financial Market Infrastructures (or PFMI) were introduced. They were to ensure that the infrastructure supporting global financial markets would become even more robust and thus be well placed to withstand financial shocks going forward.

In Europe, the PFMI were implemented in 2014 through the European Central Bank Regulation for Systemically Important Payment Systems, or SIPS, of which four were identified for Europe. In the high-value space, there are two SIPS: the Eurosystem's TARGET2 and EBA CLEARING's EURO1. In the euro retail payments space, CORE(FR) operated by STET and EBA CLEARING's STEP2-T system fulfil the SIPS criteria.

Both of those platforms had just onboarded substantial volumes during the mass-scale migration to SEPA standards completed in the first half of 2014. While this changeover had kept risk managers on their toes as well, it proved to be rather uneventful. Mainly thanks to the proficient experience that financial institutions across Europe had been able to build up over the five years following the launch of the first SEPA Scheme and of the first SEPA-compliant automated clearing house, STEP2, in 2008.

The requirements of the SIPS Regulation and the subsequent Revised SIPS Regulation, which entered into force in 2017 have had a vast impact at many levels, affecting for instance the governance arrangements and capital reserves of payment system operators. Depending on the rules and set-up of the systems, achieving SIPS compliance has also meant changing a system's credit risk arrangements, its participation criteria or its settlement model.

While work was still ongoing on finalising some of these requirements, a major incident struck in the form of the Bangladesh Bank cyber heist in 2016, focalising the attention of CROs around the world on the mitigation of cyber-related risks. In the last 2-3 years, a lot of ground has been covered towards standardising the industry's approaches to mitigating cyber risks, reinforcing end-point security and strengthening data protection and security. These efforts have been taken forward both at pan-European and global level, and both by overseers and by private industry players. Examples of relevant initiatives for European players are the ECB's Cyber resilience oversight expectations for FMIs, an ECB-lead Euro Cyber Resilience Board for pan-European FMIs, their critical service providers and public

authorities, TIBER-EU, a joint initiative of the ECB and EU National central banks and SWIFT's Customer Security Programme.

With this reference to cyber-related risks, I am completing my short historical tour of the leading trends in payment systems risk management over the past three decades. Although William Faulkner argued that the past is never dead and not even past, I believe we all agree that it is much easier to discuss trends in retrospect because they have already unfolded and many of their consequences have become apparent. For the present and future, this is not the case. That's why all I can do here is dig into the complexity for a few minutes and try to identify a few highlights:

As the agenda of today's symposium confirms, the global move to real-time payments is a big topic for CROs across the whole ecosystem. The accelerated transaction pace is posing new challenges to the screening systems of financial institutions. But at the same time, the availability of real-time messaging also opens new opportunities to tackle these challenges, thanks to emerging solutions like request to pay or request for payment, as it is called in the US.

We will also hear more today about current risks in high-value funds transfers. Developments in HVP systems these days are very much shaped by the global migration of these systems to the ISO 20022 standard, which is to be completed in 2025. As a seasoned European Payments Executive recently put it, "[this] is probably the most impactful payments industry undertaking since the introduction of the Single Euro Payments Area more than a decade ago. It will require CEO commitment, allocation of appropriate budgets, resources and project teams given that a multitude of areas will be affected across institutions." I would like to add to this statement that unlike SEPA migration, however, the European changeover will be conducted in a big bang approach, which comes with different risks and challenges.

Another hot risk topic is third-party risk management and compliance, of which the present agenda addresses a highly relevant aspect in the third session: the relationship of banks and fintechs and its impact on risk management throughout the payment systems. There are many more risks to be considered under the third-party risk headline though: open banking and access to payment accounts and data by third-party providers – and even subsequent providers – for instance. With PSD2, the latter has recently become mandatory in continental Europe and is still struggling with a number of teething problems.

But the list of third-party risk topics does not stop there: incumbent operators have to take new and future payment systems by non-traditional players into consideration. And every now and then, and more frequently these days, there is a need to manage the collateral damage of those moments where payment systems are suddenly dragged into the limelight of international politics.

And, last but not least, there is a changing supplier landscape to be reckoned with in a world where we have a cloud service alternative for everything. A world where cost-minimising bank-owned system operators are also faced with a rapidly consolidating supplier market, which has reached unprecedented levels of market capitalisation.

From third-party provider risks, we could move on to technology-related risks and the question of how we can best combine the stability of today's payment systems with the agility of tomorrow's technology – or should I better say: the stability of the current payment systems with the agility of today's technology. There is no doubt that the technology race is on. And if you recall what I just told you about third parties a minute ago, payment system operators will be well-advised to partner up with suppliers that have built up the necessary resources to keep up with the pace and the investments on the AI front alone. Just think about the impact Deep Fakes might have on trust in this new world.

Together with their users, payment system operators will have to assess how to take advantage of the benefits of new technologies and standards and how to reiterate fast without jeopardising the ecosystem's stability. And with the Internet of Things, there is a least one new frontier out there calling for smart payments integration.

Increasing digitalisation, globalisation, and environmental change have further shown us that payments risk specialists of the 21st century have to be highly attuned to social, political and environmental developments. External factors – that is factors, that are not directly related to payments or even financial markets – can pose significant risk to payments infrastructure providers. Think of the recent wildfires and preventive power outages in California, which exposed significant shortcomings in the risk management of an infrastructure provider.

Let me wrap up with a few comments on the lessons for the future that we might learn from the past and the present. My first observation is that, in terms of payment system risk management, the past two decades had a lot in common. During these years, many of us were busy reacting to worst-case scenarios that had already become reality. As different as they were, those disasters taught us important lessons and we put a lot of effort into developing our systems operations and our risk management approaches and tools accordingly.

Now, the nineties are a very different story. Remember how I told you about the plans we were making at the time because we were preparing for the end of the world as we knew it. We actually didn't keep it to plans at the time. Industry players and stakeholders were forming new connections and coalitions. Together, they came up with new ideas and visions for the future and took the necessary steps to implement them. We had realised we needed new visions and better performing co-

operation models because we were keenly aware that the old ones would not do and that none of us could tackle the challenges of the brave new world ahead of us alone.

I firmly believe that today's situation in the payments and payment infrastructure space has much more in common with the late nineties than with the two decades we have experienced since. As the American social scientist and Nobel Prize winner Herbert Simon once concluded from his study of chess masters, accurate expert intuition is nothing more and nothing less than recognition.

Only time will tell whether my intuition is accurate and whether today's situation really is comparable to that in the nineties. But it might be worthwhile trying to apply the same cooperative spirit and the can-do attitude of those days to today's challenges.

We will have to strengthen our collaborative engagement and strike new alliances if we want to successfully combat fraud or implement payment standards to optimally serve existing and new use cases, such as in the Internet of Things context. And it will take bold collective visions and clear action plans to ensure that our co-operatively developed payment systems and our four-corner model approach to payment products continue to optimally serve the needs of our customers and the overall ecosystem.

While moving forward, our risk experts will have to manage the existing risk universe of our systems and try to get ready for tackling even the unknown. To use a famous motto from a musical, also playing here in New York, The Lion King…but not the one you're expecting…: "Be Prepared." And for the rest: "Hakuna Matata".

Thank you for your attention. Enjoy this symposium and this year's TCH and BPI annual conference.