Tuomas Välimäki: Finland's experiences with sector-wide backup solutions

Speech by Mr Tuomas Välimäki, Board Member of the Bank of Finland, at the 6th Annual Nordic Cyber in Finance Conference, Copenhagen, 26 September 2023.

* * *

Accompanying slides to the speech

I'd like to thank Danmarks Nationalbank for the great conference so far, and also for inviting me to talk about our experiences with Finnish backup solutions for emergency situations.

I will take you through the reasoning on why I think that central banks need to be involved in having sector-wide backup solutions, and also what we did in this area last year.

First, a few words on my background. I was in the Bank of Finland's Market Operations and a member of the ECB's Market Operations Committee 15 years ago, when Lehman Brothers failed. Later on, I became the head of our Monetary Policy Department and was a member of the ECB's Monetary Policy Committee at the time the euro area entered the sovereign debt crisis. So when, as a board member, I was given responsibilities that include IT and Payment Systems, I obviously held a firm view of where the next crisis would emerge! And, I was half right: it was a virus a biological one instead of a cyber one. But I'm still counting, and in the meanwhile trying to raise awareness of the need to be prepared.

You all understand that stability and crisis prevention are close to the heart of a central banker. Even if our inflation has halved to 5% from its double-digit peak last year, it's easy to forget that central banks were not originally created to ensure price stability. For example, the US Federal Reserve was established back in 1913 to prevent bank runs, which were common in the first decade of the last century.

The importance of financial stability was reinforced earlier this year. A modern bank run does not involve people queuing in front of a bank. Instead, it takes place digitally. But the origin of March Madness in the US banking sector was traditional – issues with liquidity, or more precisely, loss of confidence in some institutions' ability to meet their obligations in the future.

So how does this relate to cyber issues? Loss of confidence is a common denominator behind most systemic events. In financial markets, even solvent institutions are fragile if they run out of liquidity, and your liquidity position is guaranteed only for as long as other market players have confidence in you. To make things worse, you can be hit with a loss of confidence via contagion, even if it's not you that initially faced the problems.

Let's assume that a Finnish bank is hit by a cyber incident, and as a result its customers cannot access their accounts. It's not this bank that would face a run, as it is closed, but I am certain that the customers of other Finnish banks would be scared, and at least

some of them would run for cash. So, a cyber incident can have major externalities, which – via contagion – may easily turn into systemic problems.

Contagion and systemic characteristics are precisely the reason why we, as financial market authorities, need to be deeply involved with cyber issues. Our role in a systemic crisis is not limited to addressing liquidity problems, as we have also been given an oversight function. We are overseeing payment and settlement systems, where the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives and, where necessary, facilitating changes.

The ability to print money is handy when it comes to a traditional liquidity crisis, but when we are facing cyber incidents, it is not much help. We need thorough monitoring to identify threats. We also need common, trusted platforms to share information on detected incidents, and we must have comprehensive plans to contain the impact of incidents, and systems to facilitate a quick recovery when things go wrong.

WHY AND TO WHAT EXTENT SHOULD THE INDUSTRY BE PREPARED?

[Slide 2]

To put this all in one word, we need to be prepared. I believe we can all easily agree on that. But when we go to the next step, it gets more complicated. We all have different interpretations of what preparedness means. Not to mention the heterogeneity of the scenarios that you think you need to be prepared for. Also, the motives for preparedness differ among the various actors involved.

At an individual institution's level, preparedness usually relates to business continuity. The institution must make sure it can function as well as possible when everything is not working as planned.

When it comes to common infrastructure, there should be the preparedness to guarantee the functioning of a network of individual institutions and central connection points if something in the infrastructure is damaged.

The ultimate task for governments is to limit the damage to the functioning of society under all circumstances.

For the financial market authorities, the motivation to prepare is a combination of all this. Regardless of the scenario, our task is to ensure that the financial market services vital for society continue to function – even under circumstances which an individual company is unable to prepare for or, without official intervention, lacks sufficient incentives to do so.

WHY PREPAREDNESS BECAME A KEY TOPIC IN FINLAND

[Slide 3]

So, why did preparedness become a key topic in Finland? There have been at least three different developments that have increased the need to be prepared in our financial sector.

First, our banking sector has gone through big structural changes. Previously, preparedness activities used to be local, and the credit institutions shared common principles on being prepared. In the last 20 years, there has been a shift from local services and IT systems to international ones, both within financial institutions and across payment services. This has meant that cooperation in the financial sector, when it comes to preparedness activities, has become increasingly based on information sharing. Important, of course, but simply not enough.

Second, technological development. New technologies and ways of providing financial services, such as online banking and cloud services, have been introduced. Hand in hand with the obvious benefits come new risks as well. The financial sector consists of complex outsourcing chains that are difficult to manage. Outsourcing can also lead to concentration risks, where one or a few service providers can become critical for the industry. Therefore, understanding the complete value chain and the infrastructure in financial services is vital.

And third, the geopolitical changes last year became the key driver for us. After Russia's brutal invasion of Ukraine, we not only reassessed our need to be part of NATO, but also the risk of cyber or hybrid attacks to our financial infrastructure. We found it necessary to increase our preparedness in the financial sector, and the retail payment area in particular.

FINLAND AS AN ISLAND

[Slide 4]

In our financial sector, many of the critical systems are located outside our borders, beyond the Baltic in most cases. This includes the core banking systems for several banks and significant elements of the processing of card payments. As for data connections, Finland is an island: we are dependent on under-sea cables.

Adding to the criticality of our international data connections, we use cash very little in Finland, which is also the case in other Nordic countries, and we don't have a domestic bank card or debit card scheme. So, most retail payments are processed via Visa/MC rails. In addition, prior to last year, we were lacking sufficient national capabilities for processing interbank payments.

Against this background, we had tried, together with other Finnish authorities, to raise awareness of the criticality of having a retail payment system that can function well under all circumstances – even if one or more banks cannot access their data for a prolonged period, or where transactions with international card schemes cannot be processed in the normal way. And for a long time, we failed in this.

Counterarguments were intuitive, such as the view that the dependency on under-sea cables should be tackled by securing the cables instead of burdening financial market

players with domestic, sometimes duplicate, solutions. Another view was that each institution should be responsible only for its own business continuity, not for its potential systemic implications.

SECURING DAILY PAYMENTS IN FINLAND

[Slide 5]

After 24 February last year this all changed. It was clear to the financial market authorities that preparedness had to be raised to the next level – especially when it comes to addressing cyber risks or being prepared for hybrid warfare.

We also understood that we cannot immediately improve all systems against a wide range of threats. So, our objective was to create and implement national fallback arrangements to secure the most critical services. Based on risk assessment, securing daily payments was recognised as the key priority.

As a central bank, we certainly understand the value of a smooth flow of financing to the economy as well as orderly functioning of the securities market. But when it comes to bolstering the resilience of society, the necessity to secure retail payments cannot be sidestepped. People simply need to be able, on continuous basis, to pay with their debit cards, make and receive credit transfers and withdraw cash.

The most urgent preparations for this consisted of legislative changes and building the technical capabilities. Urgent legislative changes were introduced to Parliament in late June of last year, and Act 666/2022 entered into force just a couple of weeks later, on 11 July 2022.

According to the new rules, the Financial Stability Authority, which is the resolution authority in Finland, maintains a National Emergency Account System that consists of two parts: the National Emergency Account Service and the National Emergency Payment Card Service.

The system is activated if and when the availability of one or more credit institutions' operating systems is prevented, leading to the unavailability of account information, or if a credit institution cannot execute interbank payments or if card payments cannot be verified or transmitted. So basically, the backup system takes over the basic banking services for a bank whose operations are critically damaged. You could consider this a restoration platform with basic payment functions. This is not to be confused with a bank under resolution, as the credit institution concerned is still financially sound, and its customer accounts and functions would be migrated back to it as soon as it is operationally viable.

The responsibility for our National Emergency Interbank Payment Scheme rests with the Bank of Finland. This is a contingency arrangement that secures interbank payments if the emergency account system has to be activated or if Finland temporarily loses its data connections to the rest of the world.

Although the legislative changes and the solutions selected were prepared at extremely short notice, the solutions were based on analysis work completed over a much longer period.

The technical capabilities were introduced soon after the legislation. For the interbank component, we decided to have a staggered approach to the process: quickly introduce a basic entry-level model, to be fully tested, improved and automatised only afterwards. This is not our normal way of adopting a new piece of infrastructure, but last year, with a war in Europe, we felt this necessary. And I must add that practically everybody in Finland understood the severity of the changes in our threat landscape. Therefore, even though the task was sometimes technically demanding and came with extra costs, basically all financial sector participants accepted the facts and went along with the common goal.

Any decision to activate the new National Emergency Account System needs to be taken by the Finnish Government. The resolution authority was chosen to maintain the emergency account system primarily because Finnish banks were already frequently providing the authority, for deposit insurance purposes, with relevant information on retail accounts. This minimised the need to build new communication channels, which can be very time consuming. The resolution authority was allowed to use external service providers to build and maintain the backup solutions. And naturally other authorities, especially the Bank of Finland, lent their expertise to these colleagues.

It was clear to us from the beginning that the Bank of Finland had to be the one to provide and operate the backup system for interbank credit transfers. This is a continuation of our normal tasks – we are the ones that operate TARGET2 in Finland. This is also why we, the Bank of Finland, decide independently on the activation of this part of the emergency backup systems. Independent decision-making also enables us to activate our backup systems in a scenario where there is a need for contingency clearing and settlement of payments even though the emergency account system has not been activated.

The authorities created the arrangement, but it is essential that Finnish banks and significant foreign branches can use the systems provided by the authorities. Thus, the legislation requires that banks make the necessary preparations to be able to access the emergency facilities. This includes relevant changes to banks' systems and processes.

Each institution is still responsible for its business continuity, but we require all parts of the network to also be prepared to do their share in ensuring systemic business continuity. To complete the picture, the emergency solution also needs to be adopted beyond the banks. For example, the major grocery store chains and petrol stations must be operationally included in the solution. Normally, I'm always worried about oligopolistic features in small economies like Finland, but from a preparedness point of view, this considerably facilitated our task last year.

QUESTIONS RELATED TO PREPAREDNESS

[Slide 6]

Today we are better prepared than we were a year ago. We have solutions to protect people against systemic level risks, but we still face many open issues. At the beginning, I referred to financial stability and the functioning of society. Based on a criticality assessment, we decided to first introduce solutions to address vulnerabilities in daily payments. This is not the end of the story, however. Once the most vital services are sufficiently secured, other parts of the financial system need to be considered.

Safeguarding capital markets from an operational point of view is another area to be addressed in the near future. How long would society be able to function without financial intermediation, and should we protect against incidents affecting our market participant access to the international market?

International services need international preparedness solutions. From our perspective, it is not a viable option to create national standby solutions for international services. National solutions should probably only be established for the most critical services and for the most extreme scenarios.

Migrating data to the cloud is becoming increasingly important for businesses, especially in times of crisis. Several Ukrainian banks successfully moved their IT infrastructure from on-premises data centres to the cloud in order to minimise the risk of data being destroyed by physical attacks. Moving data to the cloud offers several benefits, such as cost-effectiveness, data backup and lower risks to legacy infrastructure. However, there are also challenges posed by, for example, compliance with data protection laws and regulations. The assessment of whether to involve cloud services as part of preparedness solutions should probably be done on a case-by-case basis for the services and scenarios. The usefulness of cloud data may also depend on whether the data can be utilised for providing services to users.

Finding a balance between preparedness based on regulation and voluntary arrangements is also important. On the one hand, regulation enables a level playing field for all parties. On the other hand, regulation might be seen only as an enforcing factor that could hinder voluntary close cooperation and preparedness solutions in the market. This may apply especially to potential common or uniform preparedness solutions in the Nordic countries.

Finally, let me conclude my remarks by referring to CBDCs as a potential future way to increase the resilience of our retail payment landscape. The ECB Governing Council should decide next month on moving to the next phase of the preparations for a digital euro. If we are to introduce a new retail payment method in Europe, we need to design it so that it truly brings us new rails that are operationally separated from existing ones. Moreover, I believe it is necessary to take resilience issues on board right from the beginning of the project. With careful planning, a digital euro could become a key feature of a secure, resilient and efficient European retail payment landscape. It could also become a major part of our preparedness in the future.

Thank you.