Oslo, 19 February 2025

Visa consultation response on NOU 2024:21

Contents & Disposition

About Visa

Visa is one of the world's leaders in digital payments. Our purpose is to uplift everyone, everywhere by being the best way to pay and be paid. We facilitate global commerce and money movement across more than 200 countries and territories among a global set of consumers, merchants, financial institutions and government entities through innovative technologies. Since Visa's early days in 1958, we have been in the business of facilitating payments between consumers and businesses. As a trusted engine of commerce and with new ways to pay, we are working to provide payment solutions for everyone, everywhere. We are focused on extending, enhancing and investing in our proprietary network, VisaNet, to offer a single connection point for facilitating payment transactions to multiple endpoints through various form factors. Through our network, we offer products, solutions and services that facilitate secure, reliable and efficient money movement for participants in the ecosystem.

A. Summary of Visa's recommendations

Visa Europe Limited (referred to as 'Visa' in this document) is pleased to submit our consultation response to the inquiry NOU 24:21 *Trygge och enkle betalninger for alle* (the 'inquiry').

Visa welcomes the inquiry's intentions to increase civil preparedness for payments in Norway and to put in place a secure and reliable system for offline card payments for national emergency situations. We share the Government's, and the inquiry's, interest in promoting a safe, well-functioning, innovative, and inclusive ecosystem that benefits all participants. An ecosystem where digital infrastructure becomes more resilient, where innovation can progress, and where no one is left behind. This is central to our mission to contribute to security, sustainability, inclusion and positive change in the communities where we operate, by being the most trusted and secure digital network in the world.

The importance of trust in payments

Trust in payments is essential for both consumers and merchants. For consumers, it ensures their payment information is protected, reducing the risk of fraud and identity theft. This confidence encourages more purchases, boosting economic activity and growth. For merchants, a trusted payment system leads to higher customer satisfaction and loyalty, ensuring smooth and secure transactions. Ensuring a well-functioning payment landscape that leverages multiple operators, and their significant investment and contribution to cyber and operational security, helps increase the overall resilience of the financial sector in Norway. Visa's contribution through delivery of a resilient and international payment system can play a significant role in fostering this trust.

Visa's commitment to resilience in the Norwegian payment ecosystem

Visa leverages extensive and resilient cross-border infrastructure to help ensure our network remains available and can withstand multiple disturbances and simultaneous attacks. Triple-redundant global data centre infrastructure backs up Visa's transactions. If there's an outage at Visa's European data centre, transactions can be routed instantly and automatically to one elsewhere in the world and will still complete. Alternative contingencies such as satellite connectivity remain possible in extreme situations.

Visa's world-leading resilience technology and operations support a consistent connection uptime of more than 99.9999% between VisaNet and its global clients. If a

Norwegian bank that offers Visa cards has an outage, Visa cardholders will still be able to use their cards to pay and be paid because Visa can 'stand in' on behalf of the cardholder's bank to approve or decline transactions in the normal way via Visa's Smarter Stand-in Processing (STIP).

Visa has over 1,000 full-time cybersecurity specialists across the world, with a dedicated team in Europe, using neural networks to analyse petabytes of data to enable them to protect our network. At the same time, we have created Cybersecurity Fusion Centres on three continents, delivering 24x7x365 risk and cybersecurity monitoring, incident response and investigations, and threat intelligence capabilities.

We have invested over $10 billion in technology over the last five years – to keep the network running at pace, and to ensure it is evolving and harnessing the most cutting-edge innovations out there. By doing this we help to prevent an estimated $27bn in global fraud every year and incidents of fraud occur in less than 0.1% of transactions - among the lowest of all payment forms.

Visa's robust security measures, such as encryption, tokenization, and advanced fraud detection algorithms, help protect network participants from potential threats. By continuously investing in and enhancing its payment infrastructure, Visa ensures that its network remains reliable, even in the face of cyber-attacks or technical failures. This resilience not only bolsters consumer and merchant confidence in Norway but also supports the overall stability and security of the global financial ecosystem.

In summary, Visa recommends the following:

1.1 Measures to ensure adequate preparedness

- Adopt and implement industry-wide offline payment solutions that allow participation and contribution from all card networks, ensuring multiple layers of resilience, contingency and offline payment capabilities for consumers and businesses in Norway.

- Avoid creating a single point of failure in the Norwegian payment ecosystem by leveraging the resilience and offline payment capabilities of a diverse a range of payment networks, rather than relying on a sole domestic card scheme as the national solution.

- Ensure that any market intervention aimed at achieving national security objectives is proportionate to the desired outcome and does not disrupt competition or a level playing field for market operators.

- Ensure that any digital preparedness or offline payment solution is accessible to everyone in Norway during crises, including tourists, non-residents, vulnerable groups, and non-nationals.

- Apply industry learnings from similar offline payment solutions in the Nordics and Europe where multiple card networks collaborate in national offline payment solution.

Visa's recommendations in this area are further developed in Part B, page 6.

1. 2 Measures to ensure financial inclusion

- Minimize unnecessary industry costs to lower entry barriers for consumers accessing financial services.

- Integrate digital and financial inclusion goals to reflect growing digitalization and innovation, aligning on common principles such as accessibility, financial literacy, and choice for both industry and civil society.

- Implement trusted and reusable digital identities across the industry to simplify account opening, login, and authentication processes for users.

Visa's recommendations in this area are further developed in Part B, page 8.

1.3 Measures to ensure privacy

- Encourage data minimalization principles and consent to protect user privacy.

- Recognize and consider trade-offs between privacy or anonymity of a payment user as a public good, and the criminality risks carried by untraceable, cash-like payment transactions.

- Explore alternatives to developing untraceable digital payments options. If unavoidable, set very low transaction limits and restrict their use to face-to-face transactions only.

- Promote user identification and verification checks that are proportionate to the risk of the financial service; security measures should be tailored to the specific risk associated with the service, ensuring they are neither excessive nor insufficient.

Visa's recommendations in this area are further developed in Part B, page 9.

B. Main content

1.1 Measures to ensure adequate preparedness

We observe political and regulatory appetite for 'worst case' scenario solutions taking hold across several Nordic and European countries to ensure that consumers and merchants have access to important services – like making payments – in times of crisis or digital disruption. There are many benefits to leveraging digital infrastructure like Visa to enhance security and trust, including solutions which work 'offline'.

We identify several substantial risks within the suggestions of designating a single card network as a sole national solution for offline payments during disruptions and national crises. This would not benefit Norwegian crisis preparedness as it would:

- Create a single point of failure with the risk of increasing the threats to the ability to make payments in Norway in the event of disruptions.
- Reduce availability of best performers and exclude networks that offers world-leading resilience and security to Norwegian consumers and businesses.
- Exclude many Norwegian citizens and visitors to Norway who are not carrying a domestic card and leave them without possibility to purchase essential goods in a crisis situation.
- Contradict the principle of redundancy of having several layers of backup solutions to critical services in society.

We recommend any regulatory initiative which aims to increase crisis preparedness in Norway to build on one of the strengths of the Norwegian payment ecosystem, the approach that global openness and innovation lead to robust services and enhanced

resilience. Norwegian consumers and businesses benefit from a diversity in the payments market where international solutions with a global scope, world-leading expertise and large resources in resilience and cyber security compete with domestic payment platforms. This leads to a wide range of payment options for consumers and businesses where increased resilience in the payment market is stimulated.

We recommend that any new regulation and measure should be outcome focused - this means avoiding protectionist measures that risk creating new vulnerabilities and that make it more difficult for Norwegian consumers and companies to enjoy the redundancy and security functions that international payment services offer.

We strongly recommend that the Government adopt industry-wide solutions for increased preparedness, contingency and offline payment solutions in Norway where all card networks are welcome to participate. Visa and other global payment networks provide several countries with well-proven offline and crisis contingency solutions if local banks or systems are suffering from disruptions. Visa has recently taken part in market-wide initiatives to ensure national offline card payment solutions for crisis situations in Denmark, Estonia, Latvia, Lithuania and soon also Sweden, in close cooperation with governments, central banks, authorities and the financial sector. The solutions adopted are well proven, resilient, reliable and secure that enables offline card payments for essential goods during major disruptions and national crises in each country. We strongly recommend that the Norwegian government take inspiration from these neighboring countries and make sure that any national offline payment solution should be inclusive.

This would mean creating more layers of resilience and ensuring inclusion of all cardholders at the same time as it avoids the major risks involved in the suggestions of designating a single card network as a sole national solution for offline payments during disruptions and national crises.

We welcome the conclusion from the Norwegian central bank cited in the inquiry, which recommends that Norwegian citizens carry several different cards to increase their ability to pay with cards during a crisis. For this to work in practice, several card schemes must be able to participate in a nationwide fallback offline payment solution.

New measures for increased resilience and crisis preparedness should also promote competition and equal conditions in the payment market. When customers have choice about how to pay, this inherently promotes positive incentives and companies must both prioritize and invest in resilience and redundancy to maintain customer

trust. Market-led competition can create higher standards of resilience than regulation alone could achieve, as it forces companies to innovate to stay ahead, not just meet minimum standards. Competition in the payment market can be strengthened by promoting interoperability – for example by ensuring that all platforms and wallets are open and neutral for different payment options.

2.2 Measures to ensure financial inclusion

Financial inclusion requires an industry-wide discussion, and public-private partnership, to ensure that Norway's payment landscape is delivering for all. These include not just the elderly or vulnerable groups, but also tourists, foreign residents and temporary population groups who may not have access to domestic solutions.

We agree that digital inclusion is key to promoting financial inclusion and that the two should be promoted together. To achieve digital inclusion, it will be important to work closely with the industry to ensure all consumers have the confidence and skills to reap the rewards of digital solutions. We have extensive experiences working with governments, authorities and financial institutions worldwide to promote participation and inclusion in the payments market, and we would be pleased to support and share our knowledge and experience in the field to any initiative which aims at increased participation.

We believe digital mechanisms can be used to give consumers choice in how they want to pay – whether it be through card credentials or enabling access to cash in more locations. We support ensuring the availability programs to educate and encourage understanding of digital solutions, including eID services as well as availability and access of cash.

Like the inquiry, Visa welcomes the development of a state-issued e-identification at the highest level of security. We want to underline the importance of interoperability between a new state-issued e-identification and e-ID initiatives in the EU. To enable wide adoption by the private sector and the citizens and businesses they serve, we also want to emphasize the importance that an e-ID must be future-proof in the regulatory framework to be able to function with payment innovations and the development digital wallets.
Looking ahead, there will be important national implementation decisions to be made with regard to the eIDAS e-ID Wallet, including how this is issued by governments. We support the promotion of an implementation model which allows for the creation of multiple wallets which can support e-ID credentials issued by the Government in order to promote further innovation and competition in the market, to enhance use cases

and adoption alongside the Norwegian e-ID solutions that already exist.

2.3 Measures to ensure privacy

Visa supports privacy and data governance public policy initiatives that provide robust protections for consumers while also facilitating responsible innovations to improve the safety and convenience of the consumer experience. Privacy nevertheless requires trade-offs to be made against security. Protection and responsible use of payment data is central to our purpose to ensure we do not use more data than necessary to address risks which could impact payment transactions.

We welcome the inquiry suggestion that *privacy must be an integral part of the future development of new payment services* and want to emphasize the role card credentials play in providing security, privacy and anonymity at the same time as being traceable by law enforcement when needed.

Visa is committed to responsible data use. We believe consumers should be able to control their data and be empowered to manage their personal information. The Visa Data Values capture key principles to apply when engaging with consumer data. Visa has a Global Privacy Program to ensure proper safeguards be applied to personal information we collect, use and share. This is centered on key privacy principles that allow the Privacy Program to adapt alongside Visa's global footprint, taking into account industry benchmarks and best practices in addition to evolving laws and regulations.

It is important to note that there are significant differences between privacy applied to low-risk e-money products – such as not applying full name checks for gift cards under certain conditions – and total, cash-like anonymity. For all Visa payment cards our clients are always able to reasonably track transactions, regardless of the level of cardholder anonymity, to an individual if law enforcement request this. This is fundamentally different from solutions which seek to enable cash-like untraceability. If digital transactions were to be granted untraceability, on the basis that privacy is a public good, there would be no recourse for law enforcement to investigate individuals paying to support criminal activities. This in itself not only creates additional risks but could decrease trust in the digital payment ecosystem.

We therefore encourage alternatives to developing untraceable digital payments options. If, however they are explored, we recommend setting very low transaction limits and limiting their use to face to face transactions only.