

**Open For Business:
Policy-Driven
Resilience in
European Payments**

This report has been produced by Oliver Wyman at Visa's request, for the purpose of outlining where vulnerabilities could disrupt payment transactions, seeking to categorise them by potential impact, and providing insight into how these vulnerabilities could be further managed. The primary audience for this report includes participants of specific events hosted by Visa.

Disclaimer: Neither Oliver Wyman nor Visa shall have any liability to any third party in respect of this report, or any actions taken or decisions made as a consequence of the results, advice or recommendations set forth herein.

This report does not represent legal or investment advice. The opinions expressed herein are valid only for the purpose stated herein and as of the date hereof. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified. No warranty is given as to the accuracy of such information. Public information and industry and statistical data are from sources that Oliver Wyman deem to be reliable; however, Oliver Wyman does not make any representation as to the accuracy or completeness of such information and have accepted the information without further verification. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions which occur subsequent to the date hereof.

Contents

Executive summary	4
1. Resilience across European payments	5
1.1. What is payment resilience?	5
1.2. Why is digital payment resilience important?	5
1.3. Who provides payment resilience?	6
1.4. Analysing resilience risks	7
2. Resilience of the main payment value chain	8
2.1. The merchant perspective	8
2.2. The payment technology interface perspective	9
2.3. The payment service provider perspective	10
2.4. The payment network perspective	10
3. Avoiding disruptions from supporting utilities	11
3.1. Power utilities are key	11
4. Disruptions to payment network connectivity	13
5. How resilience risks manifest themselves across Europe	15
5.1. Resilience considerations in Spain	15
5.1.1. High processor concentration	15
5.2. Resilience considerations in Denmark	16
5.2.1. Geographical location of payment infrastructure	16
5.2.2. Historical design ties to card rails	17
5.3. Resilience considerations in France	17
5.3.1. Offline card capabilities and configuration of stand-in processing	18
6. Conclusion: Actions to enhance resilience of digital payments	19
Definitions	21
Appendix	22

Executive summary

In recent years digitalisation has come to transform the way we pay in Europe. When reaching to pay, many of us instinctively reach for our payment card or mobile wallet rather than cash – whether that is in our local shop or paying a foreign merchant online. We now expect a transaction to work in real-time, every time, without compromising convenience, reliability and security.

Delivering on these consumer expectations relies on a mix of technological innovation and investment in security and resilience, across the entire payment ecosystem. Innovations like contactless transactions have brought the benefits of secure convenient transactions to a wider audience, and the trend has stuck. Looking ahead over the medium term, rapid evolutions in technology will continue, further providing global and increasing numbers of local payment providers opportunities to meet shifting consumer demands. Alongside that, resilience enhancements like cryptography (token) and other sophisticated redundancy capabilities and functionality are increasingly available to providers to help keep payment transactions reliable and secure.

Within this fast and complex payments environment, providing the resilience and trust in digital payments which consumers expect will continue to be a common challenge. There are broader social questions to be considered, such as fair choice and access to digital alternatives.

Visa commissioned Oliver Wyman to draft a report, seeking to provide an additional perspective on how we categorise and mitigate vulnerabilities that could disrupt retail payment transactions – with a focus on preventative measures, and a look at some emergency fallback options to add an additional layer of trust.

Oliver Wyman's analysis has resulted in five recommendations with the potential to further the resilience of digital payments and minimise disruptions:

- 1. Payment firms should assess, and consider adopting, available products and services which can support functionality during disruptions.** Many firms offer resilience enhancing capabilities within the payment ecosystem which could be applied as part of a firm's wider risk management and resilience framework.
- 2. Identify, with a view to better understand, areas of concentration risk.** Raising awareness of potential single points of failure across the industry, which pose disruption risks, is important. To truly enhance resilience, conducting scenario testing and applying those insights to aid closer regulator and industry collaboration should be considered.
- 3. Assess the efficacy of existing regulatory frameworks.** Understanding continues to evolve over the potential cyber and third-party disruptions could have on payments, which requires existing regulatory frameworks to be regularly reviewed (and discussed with industry) to ensure they robustly address these risks.
- 4. In case of emergency, focus on essential goods and services providers.** Assess the resilience and access to essential goods and services (and those who provide them) – particularly important in the event of prolonged disruption.
- 5. Recognise the foundational role of services across industries.** Ecosystem resilience in digital payments—and beyond—relies heavily on the operational continuity of power, backup systems, and network connectivity, globally. These dependencies extend beyond the payments sector, requiring coordinated awareness and preparedness from merchants, consumers, and infrastructure partners alike. Supporting and strengthening these links is essential to ensure uninterrupted service during disruptions and to foster broader ecosystem resilience.

As we look to the future, this report aims to provide a platform for discussion to deliver the underlying trust in digital payments, necessary to support European resilience and economic growth.

1. Resilience across European payments

1.1. What is payment resilience?

For the purposes of this report, payment resilience is the capability to maintain secure, reliable, and uninterrupted transaction processing across the payment ecosystem – even during stress or disruption.

Resilient systems ensure data remains complete, accurate, and timely throughout its lifecycle – from storage and transmission to processing and delivery – while protecting against corruption, loss, unauthorised access, and delivery errors.

Achieving that ‘payment resilience’ capability encompasses both operational and cyber resilience across networks, processors, technologies, and supporting infrastructure. In addition, maintaining data integrity and resilience are equally essential to deliver operational trust, regulatory compliance, and financial stability. It requires both preventive measures – such as secure storage, consistent replication, and strict access controls – and responsive capabilities for rapid detection, recovery, and continuity in the event of failures or cyber incidents.

To deliver effective digital payments, and the economic benefits which flow from it, payment users must be able to trust that their payments will work – always. Delivering this reliability element requires all participants in the payment ecosystem to maintain resilient operations. For example, card transactions depend on the seamless initiation and approval of payments through technology interfaces, processing via networks and processors, and authorisation by account providers. Each must be able to prevent or effectively manage disruptions from a wide range of potential causes.

A failure in trusted digital payments at any layer can disrupt the entire payment chain, creating both economic and reputational risk. Such disruptions may prevent consumers from accessing essential goods and services and erode trust across the payment ecosystem. The scale of impact can vary – some disruptions affect only a single entity, such as one merchant or account provider, while others can cascade across the value chain, preventing multiple merchants from receiving payments and affecting both consumers and businesses. Certain issues can be resolved quickly, while others may cause extended outages.

Strengthening payment resilience to reduce this disruption risk is a shared responsibility across the entire ecosystem. Each participant must manage its own operational resilience to prevent and address disruptions, while ecosystem-wide resilience depends on coordination, collaboration, and collective action among all participants.

1.2. Why is digital payment resilience important?

Despite many efforts to promote integration, Europe’s payment landscape remains predominantly national with over 95% of payment volume originating from local transactions¹. Domestic payment solutions continue to have a strong presence in many markets – for instance, 60% of payments in Denmark are made through either the domestic card scheme or a local instant payment method.

In parallel, the entire Europe region is undergoing a structural shift from cash to digital payments. Since 2014, cash usage in Europe has dropped sharply from 75% to just 31% of transaction volume, while the share of physical card payments has more than doubled from 23% to 51%⁴. As referenced above, the pace of change varies significantly by country: in Croatia, cash still accounts for 73% of payments in 2024, while in the Nordics, digital payment solutions are used for 85–90% of all transactions⁵.

The result of both trends means that the mix of cash and digital payment solutions differs across national borders. Looking at digital payments specifically, in Germany and France domestic card schemes account for most card payments (74% and 64%, respectively), while markets such as the UK primarily rely on international card schemes. Instant payments have also grown steadily over the past decade to represent 6% of all European payments, with usage reaching 10–15% in some markets, such as in the Nordics⁶.

The driving factor behind national payment mix is consumer behaviour – typically shaped by convenience and trust (of which resilience and security are a fundamental part). Mobile payments and digital wallets now give consumers and merchants secure, convenient access to digital transactions. These solutions account for 15–20% of all

¹ Data provided from GlobalData and Euromonitor, 2025

² Ibid

³ Domestic scheme = Dankort, Instant payment method = MobilePay

⁴ Ibid

⁵ GlobalData, 2025

⁶ Ibid

payments in Europe today – a significant rise from their near absence in 2014⁷.

Efforts to integrate and unify these digitalisation trends have seen regulatory and supervisory authorities evolve to become an important catalyst for the development of new digital payment trends. In the European Union, common rules and coordination between supervisory authorities and central banks – such as through PISA⁸ – have enabled the development of shared solutions and infrastructure, including T2, TIPS⁹, and WERO¹⁰, to support the growth and resilience of digital payments across the region.

1.3. Who provides payment resilience?

Delivering digital payment solutions relies on a degree of interconnectivity across layers of infrastructure and solution providers and underlying third-party infrastructure – transacting digitally does not occur in isolation.

This report considers a typical transaction (grossly simplified) to comprise the main payment value chain¹¹ of

central banks for settlement, core payment infrastructure or networks for transaction processing and messaging, financial institutions, payment technology interfaces and other supporting utilities – as well as wider utility networks which supply the power or communication networks necessary for digital transactions to be processed. Achieving payment resilience requires coordinated effort and collaboration across all participants in this ecosystem.

Regulators and supervisory bodies ensure digital payment frameworks remain robust, enforce compliance with applicable laws and guidelines, and promote resilience, availability, trust, and integrity across the payment ecosystem.

Figure 1 below provides an overview of the most important entities in the payment landscape for the purposes of this report.

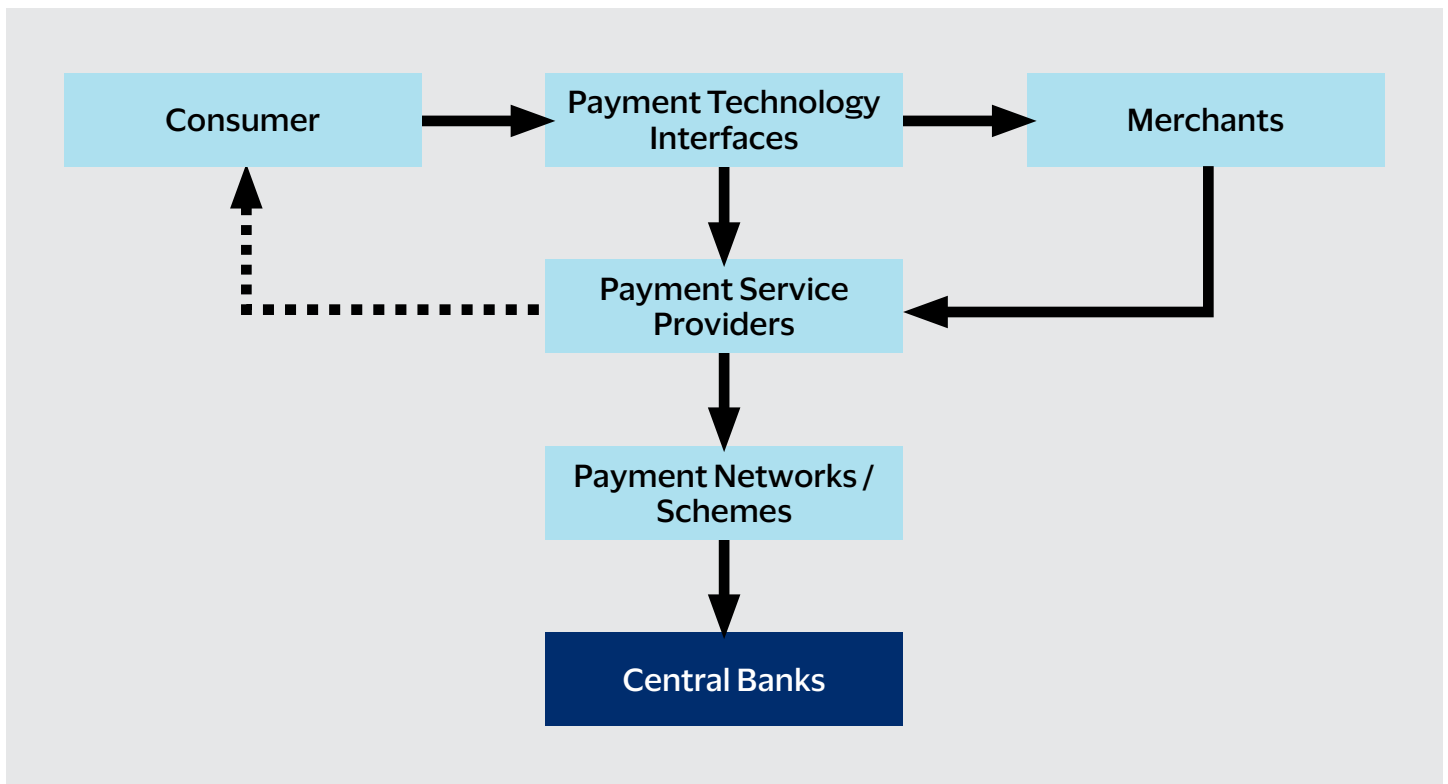


Figure 1: Payment transaction flow

⁷ Ibid
⁸ <https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews211122.en.html>
⁹ T2 and TIPS are ECB provided systems to allow for settlement of large value payments and instant payments
¹⁰ WERO is a pan-European initiative create a cross-border account-to-account solutions
¹¹ Together, the main payment value chain providers and the core payment infrastructure can be referred to as the payment value chain. See "Definitions" section for more clarifications on terminology.

1.4. Analysing resilience risks

Operational resilience risks can originate from individual payment participants themselves (e.g. component failure and other broad operational considerations), or from events which take place outside a particular participant but still result in disruption. Each of these risks and events can originate from a broad range of places – each with distinct causes, effects, and mitigation strategies.

These risks and event disruptions may prevent the routing and transfer of payment information between providers, preventing payments from being made or – if they are made without near real-time network connectivity – potentially increasing the chance of fraud.

To help provide some structure to better identify these types of risks, this report has sought to organise them against a series of headings ('archetypes'). Whilst not a recognised resilience term, structuring the information this way allows a different perspective for a non-expert audience and can look at resilience from the perspective of potential impact. These archetypes include:

Risks Originating from within an entity's direct sphere of control

- Failures in hardware, technology components, or operational processes which the participant leverages to make payments.
- Weaknesses in IT security can cause operational disruptions or compromise sensitive data, such as payment credentials. These risks include malicious cyberattacks, credential interception, data tampering, and unauthorised access, with exposure levels varying across participants.

Risks Originating from external events

- Third-party services and data integrity or availability disruptions can affect payment services and should be managed by the participant as a result.
- Power outages can disrupt operations across the entire payment ecosystem, impacting participants and services end-to-end.

Scope of potential impact

- Disruptions may be contained to a small number of entities or services or escalate into widespread outages affecting the entire payment ecosystem.

Severity of potential impact

- Impacts may range from minor (with limited financial or societal consequences) to material, posing significant risks to society or individuals – for example, prolonged inability to pay for essential goods and services.

In principle, all risks which could lead to disruption should be considered and mitigated. In practice, it is often necessary for participants, regulators and policymakers to prioritise which resilience risks to mitigate. Decision making could be guided by the level of investment required and the origin, scope, and severity of the risk for example.

Where particularly broad and impactful disruption risks are identified it may be appropriate to establish national or even European level mitigation plans rather than leaving responsibility solely to individual participants. In such cases, greater emphasis may be placed on collaborative risk reduction across the ecosystem.

2. Resilience of the main payment value chain

As shown in Figure 1, there are many participants in the payment ecosystem responsible for ensuring resilience. This responsibility includes both measures to prevent disruption from occurring in the first place, and measures to respond if an emergency occurs.

This section outlines why resilience is important for each participant in the payment value chain (as simply defined in this report) and what their primary resilience-related risks are, with a focus on operational and information security risks. Minimising disruption and outages across the main payment value chain is fundamental to ensuring that digital payments remain trustworthy, and that consumers and merchants continue to value their usage – helping deliver economic and societal benefits as are well documented elsewhere.

2.1. The merchant perspective

Merchants are at the heart of every transaction. By working with trusted payment partners, merchants can offer customers fast, secure, and convenient ways to pay. But safeguarding the payment experience also means taking steps only they can take—ensuring their systems run smoothly, protecting sensitive data, and preventing vulnerabilities from emerging.

Merchants can ensure the continuity of their payment technology interfaces and protect their customers— and other participants in the payment flow—from potential vulnerabilities, such as those arising from data storage or handling practices. Other parties (like payment service providers) can offer support, tools and guidance to help them in this effort.

Both physical and online merchants face a shared set of operational, security, and integrity risks. However, the way these risks are managed may differ, reflecting the distinct processes each uses to accept and process digital payments. By taking proactive measures, merchants help strengthen trust, protect sensitive data, and maintain the integrity of the payment ecosystem.

Exploring resilience risks

Merchants rely on many other participants in the payment ecosystem to transact, and in the case of disruption elsewhere in the payment chain, rely on mitigation solutions until normal service resumes. As a result, merchants may need to be able to react to disruptions – for example, considering how to maintain power to terminals if their usual supply is disrupted; or how terminals are set up to manage payment transactions communications in event connectivity to a payment network or payment service provider is lost.

In addition to operational risks, merchants also need to consider data integrity risks. These include taking steps to ensure vulnerabilities in the merchant’s own network connectivity setup cannot be exploited, e.g., establishing redundancies where possible to ensure payment transactions can be authenticated and authorised in case of any Wi-Fi connectivity loss. In extreme emergency scenarios, other causes of disruption – like power outages – may require risk mitigation planning to be in place to ensure payment transactions are not widely affected and trust in digital payments is not compromised. to ensure payment transactions are not widely affected and trust in digital payments is not compromised.

Case study: Spanish blackout highlighted need for robust payment contingency planning

On April 28, 2025, Spain and Portugal experienced a widespread blackout caused by failures in the Spanish electricity grid. Cascading effects from the blackout also affected telecom services, and when both power and network connectivity were lost, the payment chain was also affected. Difficulties in paying in stores occurred as point-of-sale (POS) terminals shut down either due to network connectivity issues or insufficient backup power, and ATMs also stopped working.

Meanwhile, the outage also highlighted areas where resilience is strong. For example, Visa’s deferred authorisation functionality allowed Visa cards to still be used at many merchants during the blackout, albeit with delayed processing. A similar benefit could not be provided by instant payments, which relied on live network connectivity.

The Spanish blackout incident highlighted areas where resilience could be improved. Hypothetically, at merchant and payment receiver level, increased use of backup power supply could have enabled a broader use of deferred authorisation and offline capabilities, but further analysis would be required to confirm this statement and falls outside the scope of this report. Furthermore, the blackout highlighted that providers of network connectivity should consider additional measures, for example backup power for critical hardware, to ensure that their solutions can remain operational.

2.2 The payment technology interface perspective

Why resilience should not be neglected

This paper uses the term ‘payment technology interfaces’ to capture a broad range of technology solutions that together create contingencies that can store, initiate, collect, and transmit payment credentials for further processing. The introduction of new digital payment types, e.g., instant account-to-account payments, and new technologies for storing payment card credentials, e.g., Apple Pay and Google Pay, has increased technological complexity and layering into how transaction messages flow from consumer to merchant (see Figure 1). As these technologies evolve rapidly, resilience risks are constantly changing.

By ‘collecting’ the customers’ payment credentials for further processing across the payment value chain (e.g., routing to payment networks), these interface providers¹² can be considered resilience cornerstones for the delivery of resilient payment transactions.

Exploring resilience risks

A broad range of risks have been identified relating to payment technology interfaces, including operational failure of the physical infrastructure of ‘interfaces’, e.g., payment terminals or software disruptions which may include, for example, the deployment of erroneous software, breakdown of communication protocols, and failed integration of aforementioned new technologies into existing technology stacks. An important call out is that major disruptions do not require complete failure of these elements; if no contingency resilience measure is put in place - disruption in the connection between a payment technology interface, financial institution and a payment network is sufficient to cause processing disruption and increased friction or lost consumer trust in digital payment solutions.

In addition, resilience for payment technology interfaces also includes a data integrity component, which requires a careful risk mitigation plan to be in place to ensure solutions can protect sensitive data in case of cyber-attacks. Hacker attacks can be sophisticated and global in nature, including the interception and access to payment data, theft of payment credentials (e.g., card PINs), and compromising

payment data to extract financial gain. To support resilience of this information, global payment networks invest in and leverage data encryption, cryptography (‘token¹³’) and other tools to render this information useless to criminals even if stolen.

Case study: Failure of Danish payment processor caused widespread payment ecosystem disruption

On July 19, 2025, Denmark and neighbouring Nordic countries experienced a major payment disruption due to the failure of a local card-issuing processor. The failure resulted in many merchants being unable to accept digital payments, which for those merchants not accepting cash payments caused a complete shutdown. Furthermore, the effect of the disruption cascaded into broader societal consequences as toll-bridge booths were unable to process payments, resulting in large traffic jams and long queues.

An investigation later showed that an unforeseen technical failure of a hardware component at a third-party vendor had undermined resilience efforts of the processor, as no backup was deployed for this component¹⁴. The incident highlighted the potential widespread effects that the failure of a single participant in the payment value chain can have when that participant is a widely used processor. It further highlights the need to identify all potential components and vendor relationships where the introduction of backup solutions is critical.

The incident also highlighted the need for other participants in the payment value chain to educate their users. It is not uncommon for payment networks and payment technology interfaces to deploy offline contingency solutions that merchants can use to accept card payments. However, due to a lack of knowledge of the solutions at some merchants, the impact of the incident became more widespread than it otherwise would have needed to be suggesting card acquirers have a role to play here.

¹² Payment technology interfaces include a broad range of providers, e.g., terminals (see “Definitions” for more details)

¹³ Security Token Services | Visa Token Service | Visa

¹⁴ <https://www.nets.eu/Media-and-press/news/Pages/Rare-component-failure-caused-service-disruption.aspx>

2.3. The payment service provider perspective

Why resilience should not be neglected

Ensuring strong resilience across payment service and account providers¹⁵ is fundamental for digital payments, as these entities play a critical role in ensuring transactions are processed quickly, accurately, and securely. Any disruption to their operations can impact the speed, reliability, and security of payments. If their services fail, consumers may be more exposed to disruption and fraud across their transactions – potentially reducing overall trust in digital payments.

Exploring resilience risks

These could include technology and systems failures such as core processing outages due to hardware, software, or network failures; legacy system limitations that affect scalability and speed and third-party service provider downtime, impacting transaction routing or authorisation. Payment network connectivity, fraud and transaction integrity risks, breakdowns in reconciliation, settlement or clearing processes are additional risks which require testing and redundancy measures to be put in place.

Cybersecurity threats are also important; with potential data breaches targeting cardholder or transaction data, ransomware or malware attacks that compromise systems, as well as Distributed Denial of Service (DDoS) attacks that disrupt network availability, are all of particular concern.

Other ecosystem providers, notably global card networks, offer services which can be leveraged – including stand-in processing capacity – to provide real time fraud and resilience checks using innovative AI and machine learning, alongside lowering risks of overall transaction processing disruption.

2.4. The payment network perspective

Why resilience should not be neglected

Payment networks are a critical component of the global financial system, and their resilience is essential to ensuring continuous, secure, and reliable transactions across the world. From a resilience perspective, payment networks must be designed to withstand cyberattacks, operational disruptions, natural disasters, and sudden surges in demand, ensuring that consumers and businesses can transact without interruption.

An important part of delivering reliant and resilient payment transactions is the ability of core payment infrastructure to remain operational and available to other participants in the payment chain. Different payment networks operate to different standards to resilience, with global payment networks often leading on levels of investment and network availability to other payment participants in the main payment value chain.

Exploring resilience risks

From a resilience perspective, they must be designed to withstand cyberattacks, operational disruptions, natural disasters, and sudden surges in demand, ensuring that consumers and businesses can transact without interruption. These resilience measures not only protect the integrity of the network but also maintain trust in the global payment ecosystem.

Visa, for example, invests heavily in resilience capabilities, operating multiple geographically dispersed data centres with active-active processing to avoid single points of failure. Visa employs advanced fraud detection systems, redundant network connections, real-time transaction monitoring, and robust disaster recovery protocols. In addition, Visa conducts regular stress testing and simulation exercises to prepare for high-volume transaction periods and potential disruptions, ensuring that payments can continue to flow even under extreme conditions.

¹⁵ Definition: Account providers include a broad range of entities holding consumer accounts. More in section "Definitions"

3. Avoiding disruptions from supporting utilities

Services from power and network connectivity providers underpin the whole payment value chain. Disruption to their services can cause widespread failures in the payment ecosystem through simultaneous impact across the main payment value chain. Therefore, efforts to strengthen payment resilience must address the resilience of supporting utility providers¹⁶.

This section of the paper outlines why the resilience of utility providers is an important consideration for overall payment resilience. It presents resilience risks in relation to power and network connectivity outages. Furthermore, it presents two condensed frameworks for how power and network connectivity resilience can be reviewed on a system-wide level.

3.1. Power utilities are key

Why resilience should not be neglected

Outages in power supply disrupt most of the hardware and services within the payment and network connectivity infrastructure, and consequently the ability to operate any digital payment solutions.

Exploring resilience risks

Disruptions to power utilities can occur for a range of reasons, including insufficient power generation or disruptions in the power distribution network. Depending on the nature of the distribution, the scope can range from contained risks (e.g., a power outage affecting a city district)¹⁷ to major disruptions (e.g., a power outage affecting a whole

city or a larger region). Information security breaches can impact how the power grid operates¹⁸, for example if hackers can remotely shut down parts of power generation or distribution.

Actions to enhance payment resilience further for power utilities

As power utilities are typically structured as either national or local monopolies, end-users have limited possibilities to incorporate grid redundancies into their power infrastructure. Instead, resilience should be secured at a national or regional level by considering robust power generation and robust power distribution. Table 1 below provides an overview of how resilient setups can be designed. Further complicating power generation and distribution resilience is the fact that building large-scale redundancies often requires significant investments, making such redundancies cost prohibitive for individual participants in the payment ecosystem.

Resilience consideration	Actions and characteristics which contribute to higher resilience
Robust power generation	<ul style="list-style-type: none">• Diversified power generation mix, with multiple production sites• High share of stable baseload capacity• Ability to import through cross-border cables from multiple countries
Robust power distribution	<ul style="list-style-type: none">• Transmission networks with multiple pathways to prevent single points of failure• Use network designs less susceptible to disruption, e.g., underground cables

Table 1: Resilience consideration for power utility providers

¹⁶ Network and power utilities as defined in section 1

¹⁷ Localised disruptions tend to have a minor impact if those affected can leverage services in nearby districts, but for some individuals, e.g. those with restricted mobility, a power outage can introduce material risks

¹⁸ <https://www.weforum.org/stories/2025/05/spain-might-not-cyberattack-blackout-power-outage-electric-grids-vulnerable/>

Exhibit: Resilience strategy for power utilities being at the national level

Across Europe, efforts to foster integration and redundancy in energy mixes has been a long-term objective. In reality, electricity mixes and distribution systems remain nationally diverse.

For example, Sweden has a high share of flexible hydro power (~40%¹⁹ of total electricity production). France has a high share of nuclear power and other baseload (more than 80%²⁰ of electricity from baseload) and several interconnections. Portugal has a high share of weather-dependent electricity (~40%²¹ of total electricity production) and few interconnections. Denmark has a high degree of interconnectivity with other markets.

For markets with already robust power generation (e.g., France), creating redundant distribution paths might be the most prudent approach, whereas for markets with less robust power generation (e.g., Portugal), having backup power supplies (e.g. large-scale battery solutions) might be the most cost-effective.

¹⁹ IEA on electricity generation sources in Sweden 2023

²⁰ IEA on electricity generation sources in France 2023

²¹ IEA on electricity generation sources in Portugal 2023

4. Disruptions to payment network connectivity

Why resilience should not be neglected

Processing digital payment transactions with network connectivity is crucial for the resilience of the payment network as it enables parties in the payment value chain to connect in real time and perform necessary fraud and account verification checks.

As these are required at all steps of the payment value chain, and a connectivity failure at one point can potentially introduce disruption and risk into the transaction flow. If connectivity issues affect many market participants, and no redundancy measures are in place, the potential disruption risk scales upward.

Exploring resilience risks

Disruptions to network connectivity utilities can originate from a range of sources²². At their most extreme they can be caused by, for example, software and hardware failures within utility providers or from severing of communication cables. The scope and severity of failures can be contained with minor impact (e.g., failure of a local communication cable where redundancy is in place) or cause major and material disruptions (e.g., prolonged loss of network connectivity to central banks or payment networks). Disruptions to infrastructure elements shared by several providers can create regional or nationwide disruptions.

Actions to enhance payment resilience further for network connectivity utilities

Compared to power utilities, network connectivity resilience in the payment value chain benefits from the existence of multiple delivery methods in the form of land-

based communication cables²³, cellular technology, satellite technology and multiple sources of redundancy employed by market operators. Resilience is further facilitated by the possibility of using several network connectivity providers with independent infrastructure. Hence, resilience against network connectivity risks can be increased by ensuring network connectivity services are robust and that redundant network connectivity options exist. Table 2 below presents an overview of how resilient setups can be designed.

Resilience consideration	Actions and characteristics which contribute to higher resilience
Robust network connectivity services	<ul style="list-style-type: none">• Ensure access to several network connectivity providers• Use of different connectivity solutions (e.g., cable connectivity and cellular connectivity)• Physical infrastructure deployed with sufficient geographical separation• Utilise benefits of new network connectivity solutions, e.g., satellite
Redundant network connectivity	<ul style="list-style-type: none">• Remove single points of failure within cable connectivity and cellular coverage• Merchants use redundant solutions, e.g., broadband and cellular connectivity from multiple different providers• Deploy self-healing networks to automatically manage disruptions

Table 2: Resilience considerations for network connectivity utilities

²² https://ris.utwente.nl/ws/portalfiles/portal/190061121/Availability_Incidents_in_the_Telecom_Domain_A_Literature_Review.pdf

²³ Land-based communication infrastructure can be single points of failure as these are often local monopolies

Exhibit: Recognise the risk of supply chain concentrations in cloud infrastructure

Today's digital payment solutions are built using interlinked entities across the payment value chain, where shared, and sometimes unnoticed, infrastructure dependencies constitute a concentration risk.

Supporting infrastructure is one such area where several payment value chain participants might rely on services from the same provider, with cloud services as one prominent example. A few global hyperscalers hold roughly ~70%²⁴ market share, and many entities in the payment value chain can rely on the same cloud services. As central banks and other payment market participants migrate infrastructure to the cloud, the industry's exposure to hyperscalers grows. A disruption to one of the prominent hyperscalers can simultaneously cascade into disruptions at multiple payment technology interfaces, account providers, processors, payment networks, etc., across the payment ecosystem.

With Europe moving towards shared payment infrastructure, concentration risks shift from country-specific to continent-wide. While hyperscalers offer redundancy and scalability, the resulting concentration to these providers introduces potential single points of failure that must be understood and managed as part of broader network connectivity resilience. Understanding these concentration risks, with a view to testing and applying learning from these tests, can support better risk management frameworks and form the basis of a later report recommendation.

²⁴ <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/>

5. How resilience risks manifest themselves across Europe

5.1. Resilience considerations in Spain

This section presents a selected topic related to the resilience of digital payments in Spain. It does not intend to give a comprehensive view of all resilience risks in Spain or provide a list of recommended actions. Rather, it is intended to serve as a foundation for resilience discussions among market participants.

5.1.1. High processor concentration

The Spanish payment processing market is concentrated among a few providers. The market leader, RedSys, is estimated to process more than 80%²⁵ of all Spanish payments and, hence, serves as one of the cornerstones in the Spanish market. While the prominent position of the market leader is a testament to its ability to serve customer needs, a concentrated market does introduce challenges from a resilience perspective.

Firstly, merchants tend to use the same payment technology interface for all or most of their digital payment solutions (i.e., instant payments and digital card payments). These payment technology interfaces tend to use one processor and, therefore, should the contingency efforts

of this processor fail to manage disruptions, the merchants' digital payment solutions can be impacted.

The same processor might also be used as the single point of connection to the clearing and settlement infrastructure of central banks for digital payment solutions. If this processor fails, an account provider might not be able to transfer any funds.

Finally, the high dependency on one payment processor might cause payment technology interfaces to experience operational difficulties simultaneously, resulting in nationwide disruptions to merchants' abilities to accept digital payments across material parts of the national payment ecosystem and preventing merchants from accepting payments. Error! Reference source not found. provides a simplified view of how disruptions to one processor can result in multiple or nationwide disruptions to digital payments²⁶.

While this paper does not purport to solve the concentration risk in the Spanish market, the high concentration risk should be an awareness point for market participants; market participants should be aware of the high degree of shared infrastructure elements between all Spanish digital payment solutions.

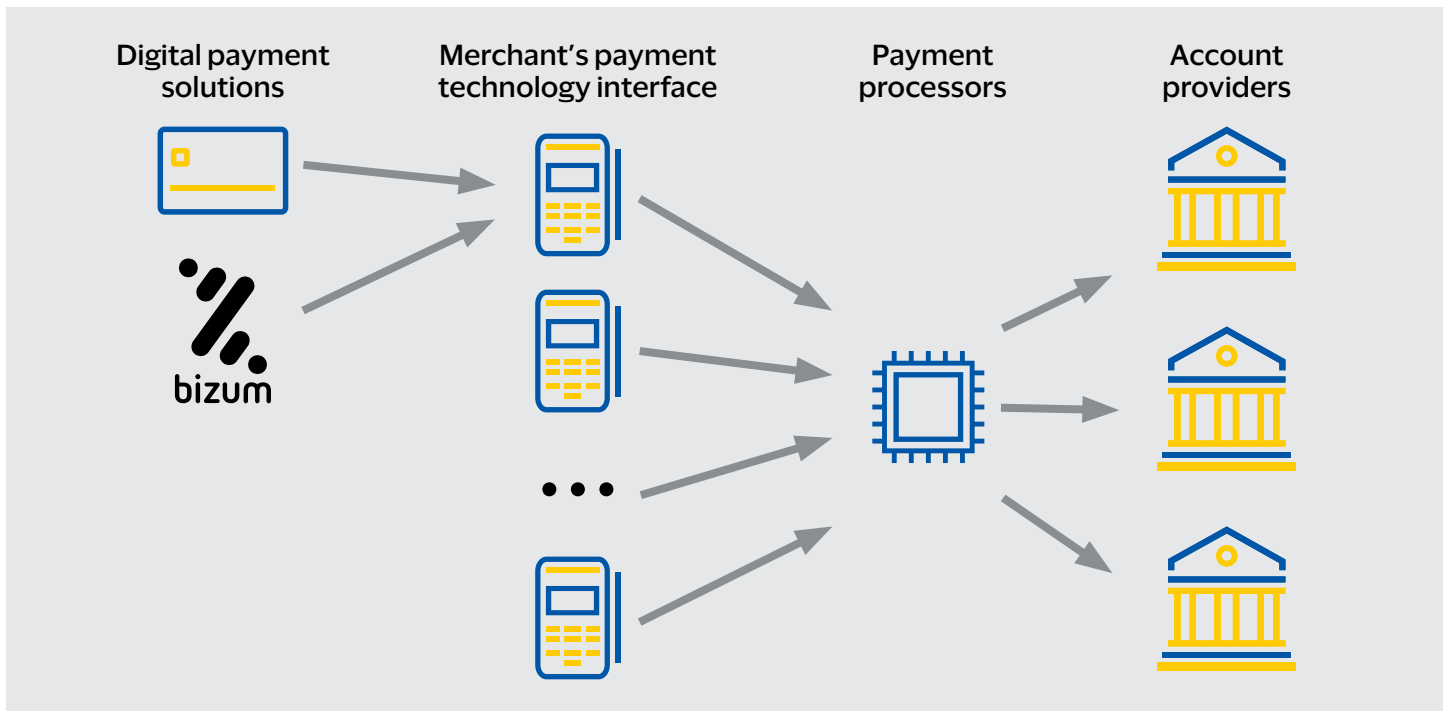


Figure 2: Simplified overview of how a payment ecosystem can become reliant on a single provider

²⁵ <https://cashessentials.org/spain-redsys-outages-bring-down-digital-payments>

²⁶ Figure 2 provides a simplified view of the value chain for card payments and account to account payments. It excludes several infrastructure elements, e.g. card schemes, and bundle other elements e.g. acquiring processing and issuing processing.

5.2. Resilience considerations in Denmark

This section presents two selected topics related to the resilience of digital payments in Denmark. It does not intend to give a comprehensive view of all resilience risks in Denmark. Rather, it is intended to serve as a foundation for resilience discussions among market participants.

5.2.1. Geographical location of payment infrastructure

The Danish payment market is characterised by a high share of digital payment solutions and little cash use. All digital payment solutions have one thing in common: they require clearing and settlement services from central banks to transfer funds between account providers. Furthermore, in 2025 Denmark decommissioned the domestic settlement platform Kronos2 in favour of the pan-European TARGET initiative²⁷.

This change introduces geographical resilience as a new resilience dimension to Danish digital payments. While the change to TARGET offers a geographically dispersed and redundant infrastructure, it also implies that all digital payment solutions in Denmark partly rely on international technology solutions. Figure 3 below show whether

different technology components used to enable digital payments are located inside or outside of Denmark.

The geographical resilience risks can cause major disruptions with material consequences to the Danish system. Disruptions, malicious or not, to TARGET infrastructure (e.g., data centres or undersea network connectivity to Denmark) risk causing prolonged outages of digital payments. Hence, ensuring contingency solutions for digital payments becomes critical.

The opportunities to provide resilience against network connectivity disruptions vary by digital payment solutions. Due to regulatory requirements for very fast settlement, instant account-to-account payments might have difficulty participating in contingency efforts²⁸. Digital card payments, Dankort, and international card schemes can provide contingency solutions through efforts such as offline acceptance or deferred authorisation²⁹. International card infrastructure further incorporates redundancies, e.g., overlapping data centres with multiple independent network connectivity routes.

We do not put forward any recommendations as to the implications of the increased internationalisation of the Danish payment infrastructure. However, market participants, merchants, and, to some extent, consumers

	Central banks	Payment networks	Account providers	Payment processors	Payment technology interface
Domestic scheme (Dankort)	International	Domestic	Domestic	Domestic	Domestic
International card schemes	International	International	International + Domestic	International + Domestic	International + Domestic
Instant payments (MobilePay)	International		Domestic	International + Domestic	Domestic

Figure 3: Primary geographic location of payment infrastructure for different digital payment solutions used in Denmark.

²⁷ Transition from charging in Kronos2 to charging in TARGET DKK, Nationalbanken

²⁸ 2023 SCP Inst rulebook, European Payment Council

²⁹ See the Appendix for an overview of contingency solutions.

5.3.1. Offline card capabilities and configuration of stand-in processing

Merchants need resilience measures to accept card payments during digital payment disruptions. Meanwhile, card schemes provide contingency solutions for disruptions of both acquirers (part of payment technology interfaces) and issuers (part of account providers). Figure 5 exemplifies different contingency measures across the payment value chain. Please note that payment networks and account providers are primary actors in this scenario, payment processors and payment technology interfaces react to the disruption instructions they receive from them.

When card issuer operations are disrupted, solutions such as Visa’s Stand-In Processing can help maintain transaction continuity. To use this solution, issuers instruct and configure Stand-In Processing for each financial institution, and payment card. That involves them introducing authorisation parameters, risk thresholds and decline codes as well as sharing cryptographic keys with Visa. Without these steps, card payments remain more vulnerable to disruptions than necessary.

Similarly, when acquiring operations are disrupted, contingency measures such as deferred authorisation and offline authorisation can be used. To be effective, these require two conditions: merchants must be aware of the contingency measures and also know how to activate them during disruptions.

Strengthening card payment resilience is especially important in France, where card payments account for over 60%³² of domestic payments. For the 80–100 million³³ tourists visiting each year, cards are often the only available digital payment method.

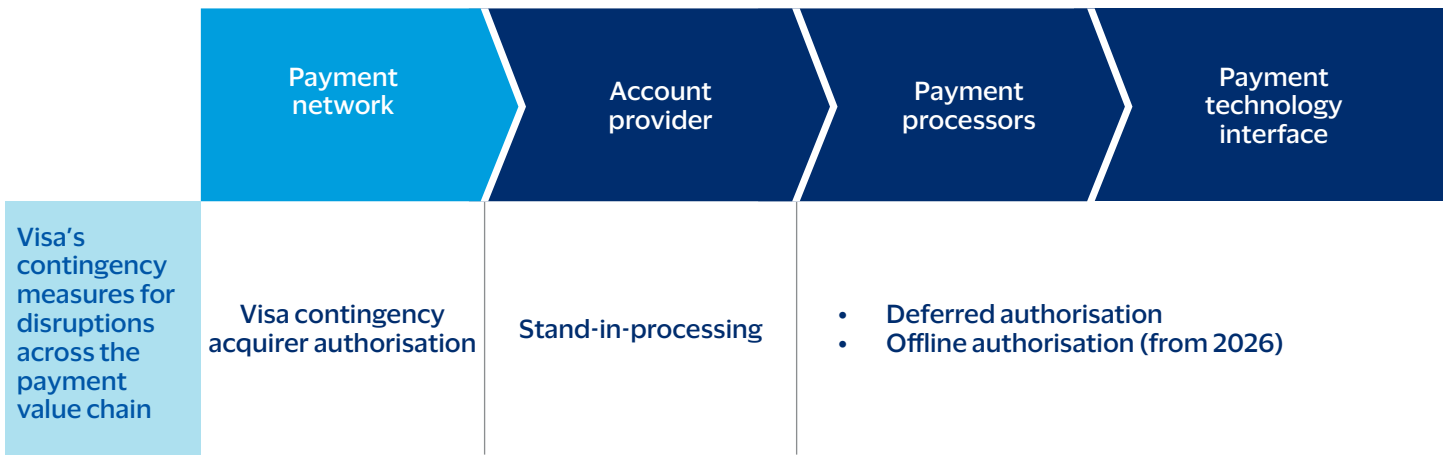


Figure 5: Visa’s contingency measures across the payment value chain

³² Observatory for the security of payment means, annual report 2023, Banque de France (2023 latest available)

³³ World Tourism Barometer 2024 & <https://roadgenius.com/statistics/tourism/france/2024-forecast/>

6. Conclusion: Actions to enhance resilience of digital payments

Accelerated digitalisation of payments across Europe has delivered substantial benefits—greater efficiency, convenience, innovation, and security. However, this has also introduced new complexities and vulnerabilities that require coordinated, ongoing action to maintain the integrity and reliability of the payment ecosystem. Building long-term resilience is a shared responsibility, demanding proactive engagement from all market participants and policy makers.

Based on the analysis throughout this paper, we offer the following five key considerations as a framework for strengthening payment resilience, accompanied by further actionable suggestions:

Payment firms should assess, and consider adopting, available products and services which can support functionality during disruptions.

In seeking to prevent and manage payment disruptions, stakeholders should consider adopting new technologies that enhance resilience across the value chain.

- Digital card schemes have made capabilities available which support standing in for other payment participants to further low-risk transaction processing in event of service interruptions to reduce disruption. Digital instant payment solutions and online payment technology interfaces do not always offer comparable capabilities.
- How participants interact across the ecosystem should be assessed with a view to identifying opportunities to encourage enhancing overall payment resilience, including through i) harmonising standards and protocols to support interoperability between digital card payments and instant payment solutions and ii) encouraging stakeholders to assess whether there are available products and services that provide additional redundancies in the event their own systems are down - such as stand-in processing or similar alternatives - across their payment mix.
- Policymakers could also explore what is required to develop robust technological solutions for managing disruptions in network connectivity to account providers; for example, considering whether SEPA regulation could allow for temporarily extended processing times or a 'deferred authorisation' approach for instant payments.

Identify, with a view to better understand, areas of concentration risk.

- Overreliance on a single or a small number of entities, or technologies, within the payment value chain can leave the entire system vulnerable. Any disruption to these cornerstones may impact even the most robust resilience efforts of other individual participants.
- Raising awareness of potential single points of failure across the industry, which pose disruption risks, is important. It is therefore vital that stakeholders consider not only the technical safeguards in place but also how collaborative efforts and targeted scenario testing could strengthen coordination at critical points of concentration within the ecosystem.
- To truly enhance resilience, conducting scenario testing and applying those insights to aid closer regulator and industry collaboration should be considered.

Assess the efficacy of existing regulatory frameworks.

- Regulators should continuously assess the effectiveness of new regulations, e.g. EU Digital Operational Resilience Act (DORA), which strengthen the obligation to review and enhance operational resilience.
- As a secondary issue not directly related to individual entities operational resilience, but which increases if ecosystem resilience is not well managed, review if the current regulatory frameworks are sufficiently nuanced to ensure that costs of fraud are handled equally between different digital payment solutions.
- Furthermore, it is worth questioning whether consumers fully appreciate the resilience risks that come from relying exclusively on a single payment method or device, such as mobile payment cards and digital wallets. Responsibility for ensuring that consumers are properly informed about these risks should be clearly defined.

In case of emergency, focus on essential goods and services providers.

- To prevent panic and widespread disruption, it's crucial to keep essential goods and services accessible during power and network outages. For some vulnerable groups, a prolonged outage can seriously affect health and quality of life.
- Hence stakeholders should consider whether essential providers should be enabled – or even mandated – to deploy resilience solutions, e.g. large battery backups, dual network connectivity solutions or alternative processing options if network connection is disrupted.

Recognise the foundational role of services across industries.

- Ecosystem resilience in digital payments—and beyond—relies heavily on the operational continuity of power, backup systems, and network connectivity, globally.
- These dependencies extend beyond the payments sector, requiring coordinated awareness and preparedness from merchants, consumers, and infrastructure partners alike.
- Supporting and strengthening these links is essential to ensure uninterrupted service during disruptions and to foster broader ecosystem resilience.

Ultimately, no single entity can guarantee the resilience of the payments ecosystem in isolation. Industry-wide and cross-sectoral collaboration, guided by clear national and European strategies, is essential.

Stakeholders are encouraged to participate in joint working groups, share incident data, and harmonise risk assessments to maximise collective preparedness. A culture of shared responsibility—where every participant from merchants to technology providers, financial institutions to regulators, and utility companies to consumers—recognises and acts on their role in safeguarding payment continuity, is fundamental to protecting trust and promoting sustainable economic growth in the digital era.

Furthermore, digital payment resilience must sit in a wider societal conversation about the role alternatives to digital payment solutions can play in light of current trends – and in terms of overall payment resilience. These considerations fall outside of this report but are worthy of further investigation.

Definitions

Account provider: An umbrella term for banks/financial institution/fintech or anyone else providing bank accounts to merchants or consumers and issuers of payment solutions (E.g., BNP Paribas).

Account-to-account payments (A2A): Electronic transfers of funds directly from one bank account to another.

Card scheme: Payment network based on card payment solutions.

Co-badged card: Payment card that can be used at multiple different card schemes.

Digital payments: Transactions where money is transferred electronically between parties using digital devices or channels, such as cards, mobile apps, or online platforms.

Global payment landscape: An umbrella term for any references to payment 'markets' outside of the national or European payment 'markets'.

Instant payments: payments that are settled immediately.

Mobile/digital wallet: Technology solution that stores payment information and enables users to make electronic transactions using smartphones or other digital devices.

Payment ecosystem: An umbrella term for the collection of financial institutions, fintech providers, technology providers, service providers which together create an ecosystem which allows digital payments to be made.

Payment landscape: An umbrella term for any references to national or European payment 'markets'.

Payment network: Organisation that provides common infrastructure and rules for processing transactions made with digital payment solutions, facilitating communication and settlement between account providers, payment technology interfaces and merchants.

Payment processor: Tech company supporting transaction data transmission between merchant, financial institution and payment network, including card payment network (E.g. Stripe).

Payment service providers (PSPs): A third-party intermediary that enables consumers and merchants to make and receive electronic payments via interfaces.

Payment technology interface: An umbrella term for providers that enable and manage the front-end experience of payment initiation and customer authentication, e.g., PSPs and gateways.

Payment value chain: Umbrella term for main payment value chain participants and core payment infrastructure (see section 1).

Appendix

Table 3 below describes the different contingency initiatives that Visa has implemented for card payments. By using these solutions layers of resilience are created, as different participants in the main payment value chain can stand in for each other. Together these allow the payment value chain to better manage disruptions to card services.

Visa contingency measures	Definitions
Deferred authorisation	<ul style="list-style-type: none">• Allows transactions to be processed even when network connectivity is lost, with formal authorisation completed once systems are back online.• Keeps merchants operational during short-term outages but may introduce elevated fraud and liability risks for longer crises.
Stand-in processing (STIP)	<ul style="list-style-type: none">• If a card issuer cannot authorise transactions due to a technical failure, Visa temporarily approves or declines payments on their behalf.
Visa Contingency Acquirer Authorisation (VCAA)	<ul style="list-style-type: none">• In the (exceptional) case all Visa data centres are offline, registered acquirers are empowered to authorise transactions on selected merchant category codes (MCCs).• Visa provides financial protection for transactions processed in this way to mitigate risk for acquirers and merchants.
Offline Chip and Pin Authorisation	<ul style="list-style-type: none">• Enables transactions to be securely authorised by the card's chip when no network connection is available.• Typically for essential categories only, with spend limits and PIN checks applied.• Applicable for longer-term outages and crisis situations• Pending launch (expected 2026).

Table 3: Contingency measures applied by Visa³⁴

³⁴ Overview of contingency measures provided by Visa

