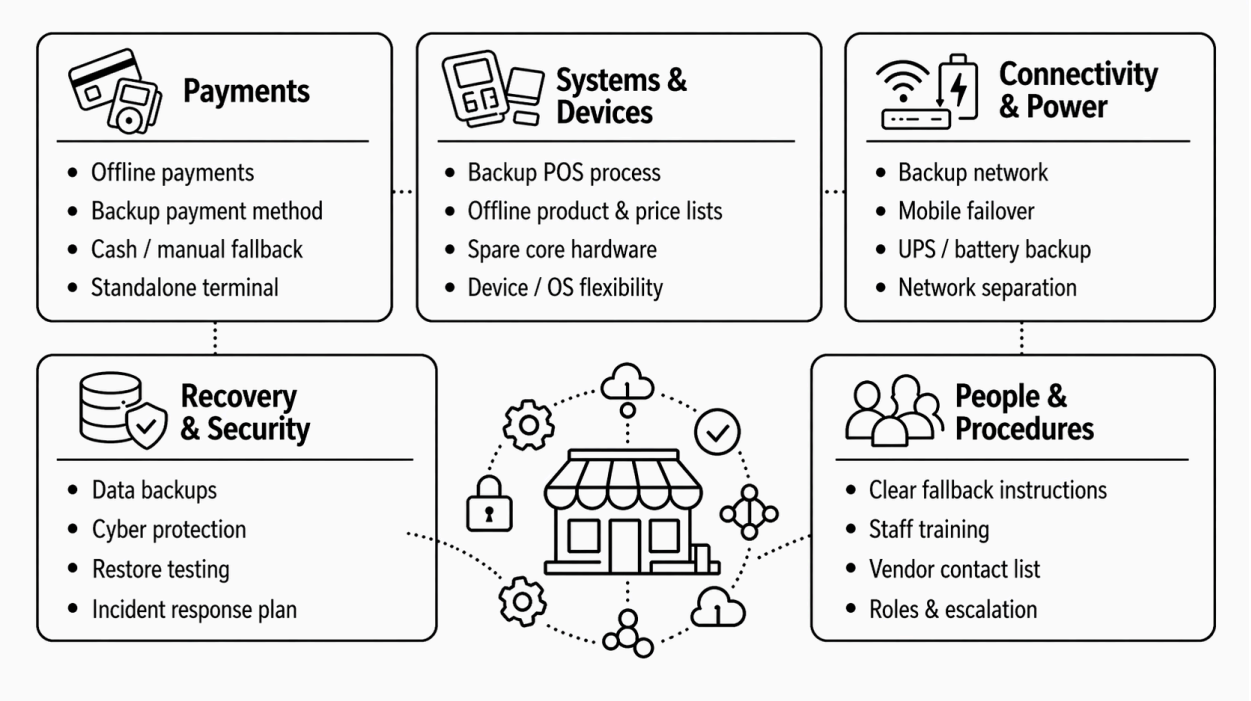
NAVIGATING PAYMENTS DURING CRISIS: TRENDS AND STRATEGIES

About D2 Group

D2 Group is a resilience technology company helping retailers, payment providers, and critical-service operators prepare for disruption. Through reports, lectures, workshops, and advisory work, D2 Group shares knowledge, best practices, and practical resilience strategies for keeping essential services available when normal infrastructure is degraded or unavailable. D2 Group's resilience framework covers five operational areas:



About this study

This report is based on D2 Group's ongoing work on resilience, including market research, stakeholder conversations in 2026, international comparisons, and analysis of emerging offline-payment models. The report focuses on practical strategies for maintaining essential retail commerce during disruptions, with particular attention to Sweden's 2026 offline-payment initiative. D2 Group believes resilience is an important issue for Sweden and aims to contribute knowledge, practical perspectives, and solutions that support a more resilient society.

Executive Summary

Sweden is entering a new phase in payment resilience. After decades of rapid digitalisation, the country now faces a strategic question: how can society keep commerce functioning when digital infrastructure fails?

The issue is no longer theoretical. Cyberattacks, power outages, war in Europe, hybrid threats, telecom disruptions, and cloud dependency have made payment continuity a matter of national preparedness. The Riksbank and market representatives have agreed that offline card payments for essential goods should be possible for up to seven days no later than 1 July 2026, focusing on groceries, pharmacies and fuel. Importantly, the offline mandate has also encouraged other retailers to implement offline functionality, including Systembolaget (alcohol retailer).

This report examines what “resilience” means for consumers, retailers, banks, payment schemes, POS suppliers and society. It compares Sweden’s emerging offline-payment approach with international models such as earlier European stored-value card systems, Hong Kong’s Octopus, and the future potential of central-bank digital currencies and stablecoin-based settlement.

The core conclusion is that Sweden should not treat offline card payments as a narrow technical compliance project, but as the first layer of a broader digital payment-resilience roadmap. The next phase should extend the discussion to mobile wallets, local stored value, bank-to-bank settlement, and future public digital-money infrastructure. If designed with offline functionality and convenient in-store use, the digital euro could eventually become part of this resilience toolkit. The objective should be to ensure that essential commerce can continue even when parts of the digital infrastructure fail.

1. WHY PAYMENT RESILIENCE MATTERS

1.1 Introduction: From cashless success to resilience challenge

For many years, Sweden's payment market has been shaped by speed, convenience, and digital adoption. Cards, Swish, contactless payments, self-checkout, and mobile wallets have transformed everyday commerce. In normal conditions, this has worked exceptionally well.

But crisis changes the payment question. The most important question is no longer "What is fastest?" but rather:

Who can still pay when systems stop working?

If power fails, if a telecom network goes down, if a bank is unavailable, if a card issuer cannot be reached, if a cloud-based POS platform loses connectivity, or if a consumer's phone battery dies, the payment system must still support essential commerce. Payment resilience is not a speed problem; it is a continuity problem.

1.2 The meaning of beredskap

The Swedish term **beredskap** captures this broader responsibility. It is often translated as "preparedness" or "resilience", but in payments it means something very practical: the ability for people to buy food, medicine, fuel, and basic goods during disruption.

That ability depends on more than one actor. Consumers need usable payment instruments. Retailers need operational checkout systems. Banks and card issuers need risk models that allow transactions to continue when online authorisation is unavailable. POS suppliers need architectures that support degraded operation. Society needs redundancy.

1.3 Threat landscape: from outages to hostile action

1.3.1 Operational failures

These include ordinary system outages, network failures, software bugs, cloud-service interruptions, and terminal connectivity problems. They may be limited in scope but can still disrupt commerce at scale if many retailers rely on the same infrastructure.

1.3.2 Criminal cyberattacks

Retail chains, payment processors and service providers are attractive targets. Ransomware or denial-of-service attacks can take down individual chains or critical suppliers. Several Swedish retail and service chains have experienced ransomware-related disruption in recent years.

1.3.3 State-level and hybrid threats

The more serious scenario is hostile action by state-linked actors. A state actor may have the capability to target banks, telecom infrastructure, power systems, or multiple parts of the payment chain simultaneously. This is the “elephant in the room” for Nordic preparedness.

Sweden and Norway have both reconsidered aspects of their cashless trajectories in light of war in Europe, cyber threats, and broader security concerns.

1.3.4 Lessons from Ukraine

Ukraine also provides concrete examples of how long and how widely communications can be disrupted.

On the first day of the Russian full-scale invasion of Ukraine, the Viasat KA-SAT satellite broadband attack affected several thousand users in Ukraine and tens of thousands across Europe; because many modems were disabled, restoration required replacement hardware for some customers rather than a simple network restart.[1]

In March 2022, Ukrtelecom, the national fixed-line operator, suffered a cyberattack that caused a roughly 15-hour outage.[2]

In December 2023, the cyberattack on Kyivstar, Ukraine's largest mobile operator, affected roughly 24 million mobile users and over 1 million home internet users; services were disrupted for multiple days, with recovery taking place gradually rather than instantly.[3]

On the morning of 26 August 2024, Russia launched more than 200 missiles and drones in one of the largest aerial assaults on Ukraine, primarily targeting the country's energy infrastructure. The attack caused sudden power outages **affecting 8 million households**, while Kyiv experienced its first unplanned blackout since November 2022.[4]

These examples are important because they show that wartime communications failures can last far longer than the short outages normally assumed in retail payment contingency planning. They also show different failure modes: Kyivstar and Ukrtelecom demonstrate hostile cyber operations against telecom providers; Viasat shows how a communications dependency outside the national telecom network can still affect Ukraine and Europe; and the repeated blackout periods show how attacks on electricity infrastructure can cascade into mobile and internet outages even where telecom assets are not directly struck. For Nordic payment preparedness, the lesson is that offline payment capability should be

[1] viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/
[2] datacenterdynamics.com/en/news/ukraine-ukrtelecom-hit-by-15-hour-outage-due-to-cyberattack
[3] wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru
[4] iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack

designed for multi-hour to multi-day degradation, not merely brief interruptions in terminal connectivity.

1.3.5 Starlink and satellite connectivity

Some businesses can use backup SIM cards from alternative network providers, while others may complement this with satellite connectivity such as Starlink. Ukraine also shows the limits of satellite backup: Starlink availability is not universal and may be restricted by geography, policy, or security considerations. For example, Starlink's company policy has made the service unavailable over the occupied Crimea peninsula.

2. SWEDISH OFFLINE-PAYMENT CHALLENGE

2.1 The 2026 offline-card mandate

The Riksbank's 2026 initiative marks a significant shift in Sweden's approach to payment resilience. It recognises that a highly digital payment market also requires offline capability. The Riksbank describes offline payments as necessary in situations where normal checks cannot be carried out, for example when internet connectivity is unavailable. In such cases, the transaction must be processed with chip-and-pin, without the usual real-time authorisation flow.

The agreement currently focuses on offline card payments for essential goods, with a target implementation date of 1 July 2026. The six largest card issuers are participating in the project (Danske Bank, Handelsbanken, Länsförsäkringar, Nordea, SEB, Swedbank). The Riksbank is in ongoing conversations with the remaining card issuers.

Based on an interview conducted on April 13, 2026 with relevant members of the Riksbank working group, our understanding is that Mastercard supported offline, but Visa did not initially support offline payments in Sweden. Following the initiative from many European stakeholders, including the Riksbank, Visa agreed to make the necessary changes. This also requires software updates to card terminals. The risk associated with offline transactions will sit with the card issuer. Our understanding is that the project group has so far been successful and remains on track to meet the planned timeline.

This is a practical and realistic first step, but it also highlights several unresolved issues:

- Not all card issuers currently support offline transactions, with some smaller banks still remaining outside the scope, such as Skandiabanken.
- Mobile wallets are not supported in the same way as physical EMV cards in offline mode.
- Cloud-based POS systems may not have full local capability for product data, pricing, and accounting.

The mandate should therefore be understood as the beginning of a broader discussion about payment resilience, rather than the end of it.

2.2 Offline

The term “offline” is not a single state. It has different meanings depending on perspective. For the **consumer**, offline may mean:

- the phone battery is dead;
- there is no mobile data or Wi-Fi;
- a digital wallet cannot connect.

This is important because Sweden has become highly dependent on mobile-first payments. If a large share of shoppers use cards through Apple Pay, Google Wallet, Samsung Pay, or Swish, then a card-only offline solution may not protect the whole population.

Apple’s Express Mode shows that mobile devices can be part of resilience when designed correctly. Apple states that Express Mode allows transit cards and certain passes to work without waking or unlocking the device, and that power reserve may allow use for up to five hours after the iPhone needs charging. More about this below.

2.2.1 Offline for retailers

For a retailer, offline can mean something more complex:

- the card terminal cannot reach the acquirer;
- the POS cannot reach the cloud;
- product data cannot be updated;
- prices and promotions are unavailable;
- inventory cannot be synchronised;
- loyalty systems fail;

- accounting entries must be created later;

This is especially challenging for chains with large SKU counts. A grocery store may have tens of thousands of products. A sports, electronics, or fashion retailer may have hundreds of thousands or millions across its broader inventory. Keeping all data locally available, synchronised, and secure is expensive.

The trend toward cloud POS makes this more difficult. Many modern retail systems were designed for always-online operation. Resilience requires a hybrid model: cloud-first in normal conditions, but with local fallback for critical checkout functions.

2.2.2 Offline for society

For society, offline means the ability to preserve commerce under severe disruption. This may include cyberattacks, sabotage, banking outages, telecommunications failures, electricity interruptions, or military crisis. In this context, payments are part of civil defence. A country cannot maintain social stability if people cannot buy food, medicine, fuel, or transport.

The war in Ukraine illustrates this point. Mikael Björknert, the Swedish CEO of PrivatBank, Ukraine's largest bank, shared how in parts of Kherson that were temporarily occupied: *"Our branches operated, hidden from the [Russian] occupiers, to ensure that the hryvnia did not disappear and that the Russians could not impose the rouble"*. Loading ATMs with Ukrainian hryvnia at night was not only a practical measure to maintain access to cash. It also helped preserve the use of Ukraine's national currency and served as a visible signal of institutional resilience and sovereignty.[5]

Offline payment capability should therefore be understood as part of a wider societal resilience framework. Its purpose is not only to keep individual transactions functioning,

[5] thebanker.com/content/06ec7266-697f-479e-b4ab-f92977e04501

but to support continuity, trust, and public order during periods when ordinary infrastructure cannot be relied upon.

2.3 Cash: necessary but insufficient

Cash remains the simplest offline payment instrument. It does not require electricity at the point of use, network access, a bank app, or a functioning card terminal.

But Sweden's cash infrastructure has weakened significantly. The Riksbank reported that the average value of banknotes and coins in circulation in 2024 was about SEK 57 billion. By contrast, Riksbank material shows that cash in circulation was SEK 114 billion at the end of 2007. This means Sweden has far less cash in circulation today, despite a much larger economy and population.

Cash should therefore be treated as a resilience layer, not a complete answer. It is critical for inclusion and crisis preparedness, but it cannot alone support the full volume of modern retail payments if digital systems fail for a prolonged period.

2.4 Mobile wallets and the missing resilience layer

One of the most important practical questions is whether Sweden's future offline payment strategy will fully cover mobile-wallet usage.

Our interviews with industry experts state that a third of consumers now pay with cards stored in mobile wallets, such as smartphones or smartwatches. If 30–35 percent of grocery shoppers use phones or watches for card payments, resilience cannot be achieved through physical cards alone. An offline strategy that excludes mobile wallets would leave a substantial part of everyday payment behaviour outside the resilience framework.

This raises important technical and operational questions. Mobile wallets may not behave in the same way as physical EMV cards when connectivity is unavailable, and the ability to process offline transactions may depend on the wallet provider, card issuer, terminal configuration, and scheme rules. As a result, mobile wallets represent a potential missing layer in Sweden's payment resilience planning. The following chapter presents examples from other countries that may offer guidance on how this issue could be addressed in Sweden in the future.

2.5 Liability, risk, and settlement

One important feature of the 2026 offline-card mandate is that card issuers bear the risk of failed offline transactions. This should be clarified to only be valid for retailers in the **essential-goods** scope. It is very positive that the 2026 offline mandate has inspired others to implement offline functionality. For example, Systembolaget has been working on offline functionality, although it is likely to bear the offline risk itself.

This may also leave room for interpretation as some retailers supplying tools, could also sell essential kits to consumers. What if IKEA began selling survival kits, would this allow them to force the bank to hold the offline risk? Retailers need clear liability rules to make sound business decisions.

When engaging retailers on payment resilience, one practical challenge is that beredskap does not always have a single organisational owner. In some companies, responsibility may sit with legal, IT, HR, finance or store operations. In others there may be a dedicated Head of Security function.

This matters because reaching the relevant audience inside each organisation is therefore a resilience challenge in itself. For authorities such as the Riksbank, industry communication should also target Retail CEOs, CFOs, CIOs, heads of security, HR, legal

teams, store operations, POS owners, finance departments and communications teams may all need to understand the details of the Offline-card mandate. Without this broader communication, the risks of offline payments may not be fully understood inside retail organisations.

3. INTERNATIONAL MODELS AND LESSONS

3.1 Nordic comparison

Denmark and Norway have strengthened consumers' practical ability to pay with cash. Norges Bank explains that a 2024 amendment clarified that consumers **must** be offered the option to pay with legal tender in sales premises where businesses regularly sell goods or services to consumers, if other payment options are available there.

Finland is closer to the Swedish model where cash remains legal tender, but businesses may have more flexibility in payment-method design. Finnish consumer guidance stresses that essential services should offer several payment methods and should not make payment options unreasonable for consumers.

3.2 Older European electronic-cash systems

Europe has experimented with electronic cash. Examples include Sweden's "**Cash card"** system, Germany's GeldKarte, Denmark's Danmønt, the Netherlands' Chipknip, Austria's Quick and Switzerland's Cash. All of these European systems were discontinued, often because card networks, online debit, credit cards, and mobile payments became more convenient. But from a crisis-resilience perspective, their core idea has become relevant again: prepaid or stored value that can be spent locally without real-time online authorisation.

The problem was not necessarily the concept. The problem was timing, user experience, interoperability, and commercial incentives.

Here is an overview of discontinued electronic cash projects in Europe:

Country	System	Type	Launched	Ended / Current Status
Austria	Quick	Stored-value function on debit cards	1996	Ended 2017
Belgium	Proton	Electronic purse	1995	Retired in the 2010s
Denmark	Danmønt	Electronic purse card	1992	Discontinued
Finland	Avant card	National prepaid smart card	1992	Phased out in early 2000s
France	Moneo	Electronic purse on bank cards	1999	Ended 2015
Germany	GeldKarte	Offline prepaid chip wallet	1996	Shut down Dec 2024
Netherlands	Chipknip	Stored-value smart card	1995	Discontinued 2015
Norway	Mondex	Mondex implementation	1990s	Pilot/limited rollout only
Portugal	Porta-moedas Multibanco	Stored-value purse	1990s	Retired
Spain	Monedero 4B	Electronic purse	1990s	Disappeared as debit/contactless rose
Sweden	Cash	Smart-card e-cash	1990s	Decommissioned 2004
Switzerland	CASH	Stored-value chip on bank cards	1990s	Mostly disappeared in 2000s
United Kingdom	Mondex and Visa Cash	Smart-card electronic cash	1990s	Last implementations shut down in 2008

3.3 Case study: Hong Kong Octopus

Hong Kong's Octopus system is one of the most relevant international examples for Sweden and Europe. The system is owned by MTR (the company is publicly listed with the Hong Kong Government owning about 75% of MTR Corporation and the rest is held by public/institutional shareholders). The company ran the Swedish underground for a decade. Octopus is a stored-value, contactless payment system used across transport, retail, convenience stores, vending machines, parking, schools, and access-control environments. Its strength is not only convenience; it is architectural resilience. Value is stored locally on the card or secure element, and payment can be completed quickly

through NFC without requiring the same online authorisation flow as a standard bank-card transaction.

For mobile use, Octopus states that Octopus on Android, iPhone, Apple Watch does not require an internet connection when paying for transport and retail purchases, because they use NFC technology for the transaction. Internet is needed for functions such as adding a new Octopus or requesting refunds.

This distinction is important for Sweden. A mobile payment can be resilient if the value, credentials, and acceptance logic are designed for local use.

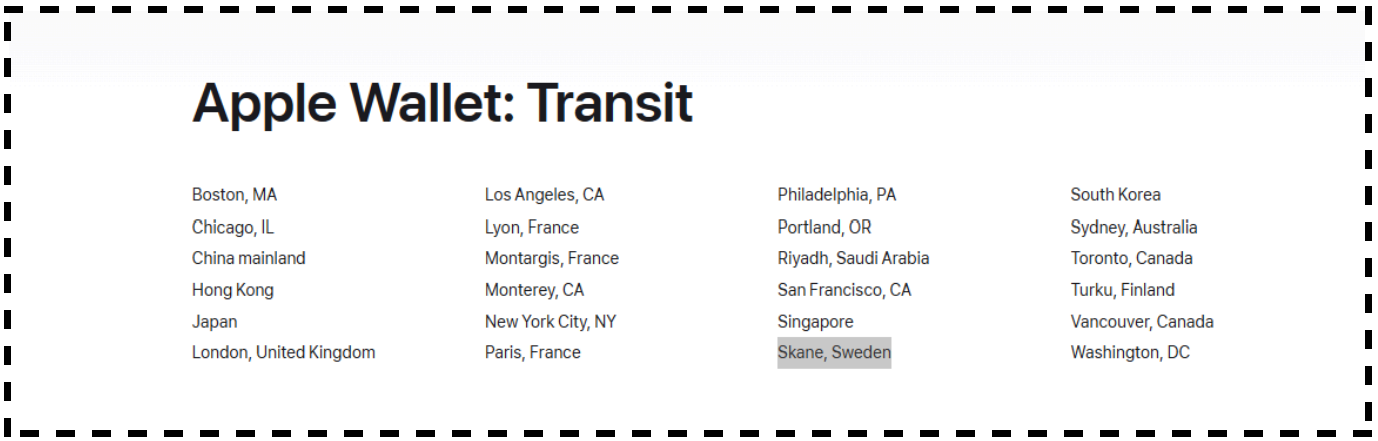
Octopus also illustrates the benefit of a dedicated low-value payment rail. It does not try to replace the whole banking system. Instead, it solves a practical problem: fast, reliable, low-value transactions in everyday environments.

For Europe, the lesson is clear: resilience may require a payment layer that is closer to “electronic cash” than to conventional online banking.

3.4 Apple Transit

One of the most interesting examples of payment resilience is already in many people’s pockets. Apple’s Transit feature shows that mobile payments do not necessarily have to depend on unlocking a phone, opening an app, or having network access. **In some cases, supported transit cards can even continue working for several hours after the phone appears to have run out of battery.** In the example of Octopus in Hong Kong, users can also use their locally stored credit with an iPhone which ran out of battery.

This makes Apple Transit a useful early example of how mobile wallets could become part of crisis-resilient payment infrastructure. Apple Wallet transit availability, accessed May 15, 2026.[6]



Many modern vehicles support digital car keys in Apple Wallet. With a compatible vehicle, this feature can be tested by adding the car key to Apple Wallet and checking that it will remain usable when the iPhone battery is depleted.[7]

3.5 Digital euro and future money

The digital euro is relevant because central-bank digital currency could eventually provide a public digital payment instrument with offline capability.

However, it should not be treated as a near-term solution for Sweden's 2026 offline-payment needs. The ECB says the preparation phase ran from November 2023 to October 2025, and that technical work and legislative support continue. If EU lawmakers adopt the regulation in 2026, the digital euro could be issued later, with 2029 described as a potential launch date, with an internal pilot exercise scheduled for 2027.[8]

[6] apple.com/ios/feature-availability/#apple-wallet-transit
[7] 9to5mac.com/2025/10/31/apple-wallet-car-key-supported-cars/
[8] ecb.europa.eu/euro/digital_euro/progress/html/index.en.html

The digital euro could become a strategically important payments solution later in the decade if it is able to compete with the convenience and acceptance of today's Visa and Mastercard products. For European merchants, the main opportunity lies in reducing the cost of payment acceptance and creating a more European-controlled payments infrastructure. However, this will only work if the digital euro is delivered through a product that consumers actively want to use. Wero Wallet, now expanding across Europe, may offer a useful reference point for the rollout of a pan-European wallet. For point-of-sale payments, NFC support should be treated as a core requirement, not an optional feature, because consumers already expect tap-to-pay functionality. The Indian digital rupee pilot, which is testing both offline functionality and NFC-based payments, could provide useful evidence on how such features perform in practice.

For now, Swedish resilience must rely on cards, cash, POS architecture, offline risk models, and possibly private-sector stored-value solutions.

Stablecoins and crypto networks are increasingly discussed in payment resilience, especially for cross-border settlement and institutional use. They may offer fast settlement and programmable money features, but they also raise tax, accounting, volatility, compliance, consumer-protection, and operational questions.

For Swedish retail crisis payments, stablecoins are unlikely to be a primary solution in the near term. Their most plausible role is in back-end settlement experiments, cross-border liquidity, or special-purpose institutional pilots. SEB is among European banks involved in a euro-denominated stablecoin initiative reportedly targeting launch in the second half of 2026. And it will be interesting to follow this initiative on how it may influence the future payment landscape.

4. SWEDISH ROADMAP FOR RESILIENT PAYMENTS

4.1 Offline cards as the first layer

Sweden should develop a layered payment-resilience model.

Consumers are encouraged to hold:

- at least two physical payment cards, preferably from different banks;
- some cash in useful denominations;
- access to more than one payment method;
- awareness that mobile wallets may not always work offline.

This aligns with the broader preparedness message that multiple payment methods improve resilience.

Retailers and POS suppliers are on schedule to implement the offline mandate in the stores selling essential goods. This will include product scanning, essential price data, payment capture, receipt generation and later reconciliation.

4.2 Next layers

Sweden should assess whether mobile-wallet transactions can be included in offline card preparedness. Swish's reported exploration of offline capabilities could also inform whether a modern stored-value layer might support low-value essential purchases. Hong Kong's Octopus provides the strongest modern reference case.

The digital euro should be monitored, especially its offline design. But it should be treated as a future complement.

4.3 Conclusion

Sweden's payment system is efficient, innovative, and highly digital. But efficiency is not the same as resilience. A payment system that works well in normal conditions must also be able to support essential commerce during disruption.

The 2026 offline-card mandate is an important first step, but it should be treated as the foundation of a broader payment-preparedness roadmap. The next phase should focus on five practical priorities:

First, Sweden should keep informing the retail industry about the liability and settlement rules for offline transactions, including how risk is allocated between issuers, acquirers, schemes, retailers and consumers when authorisation is delayed.

Second, retailers and POS suppliers should certify that offline operations work beyond the card terminal itself. Essential functions such as product scanning, local price data, receipt generation, transaction storage and later reconciliation must continue during degraded connectivity.

Third, mobile-wallet behaviour should be tested under realistic offline conditions. Since a growing share of consumers pay with phones and watches, resilience planning cannot rely only on physical cards.

Fourth, Sweden should evaluate whether a modern stored-value model could support low-value essential purchases during disruption. Earlier electronic-cash systems failed commercially, but their core resilience logic may be relevant again.

Fifth, Sweden should actively assess the digital euro as part of its longer-term resilience strategy. If the digital euro can offer a competitive consumer experience while lowering payment-acceptance costs for merchants, it could become an important complement to existing card-based infrastructure. However, this would require practical design choices

that support everyday usability, including NFC for in-store payments and robust offline functionality. Developments such as Wero Wallet in Europe and the Indian digital rupee pilots may provide useful evidence on how digital payment systems can combine scale, convenience and resilience.

Finally, the sector should rehearse multi-day disruption scenarios. Offline payments create delayed settlement, fraud-risk, accounting, and operational questions that can only be understood properly through practical testing.

True resilience requires several layers: cash, cards, mobile wallets, local POS capability, issuer risk models, stored value, and eventually perhaps CBDC.

The guiding principle should be simple:

In a crisis, people must still be able to buy what they need, and retailers must still be able to sell.

The countries and systems that succeed will be those that design payments not only for speed, but for continuity.

The roadmap below summarises the recommended next steps for strengthening Swedish payment resilience.