



How to Enable Resilient Card Acceptance Processing in the Event of Major Downtime Incidents

EPCA Forum – London

19th June 2026

Major Downtime Events – Key Resilience Questions for Large Merchants

Payment processing downtime is a store managers nightmare event. So, resilience features should be built into new architectures but are often missed out.



Major Failure Events

- EPOS update failure
- PED software update failure
- Store power outage
- Store WiFi failure
- Group network failure
- External gateway failure
- Internal gateway failure
- Store hardware component failure

Causes
&
Effects



Major Failure Impacts

- Loss of revenue/profit
- Customer confusion
- Store staff are overwhelmed
- Liability shift costs
- Restart declines
- Fraud attacks
- Increased refunds and CB's
- Compliance / regulatory sanctions

Key Observations: Using end-to-end gateway and acquiring services provided by players such as Adyen, Stripe and Checkout creates a single point of failure which concerns many major merchants!

Typical Resilience Features for Critical Supplier Large Merchant Architectures

As a result of government pressure many large merchants designated as critical suppliers in the event of serious interruptions are reviewing the resilience features within their payment systems

Service Supplier Features

-  Use of two cloud providers
-  Multiple regional data centre's ownership
-  Multi instance operations
-  99.999% uptime targets
-  Rebates for SLA failures
-  Routing to alternative gateways
-  Routing to alternative acquirers
-  High performance design features

Typical Major Merchant Solutions

-  Use of an Orchestration Supplier
-  On 'prem' front-end operations
-  Separate supplier for e-comm and in-store
-  High penalty fine SLAs
-  Battery-supported EPOS / PEDs
-  Wired group networks
-  Boosted in-store WiFi
-  Consolidation/backup in-store processor

Key Observations: Reengineering legacy components to improve resilience is complex and expensive. Many merchants chose to re-architect and go out to RFP and buy a modern service.

Option 1 – Multi ‘Supplier’ Gateway / Acquiring Architecture

Multiple Supplier Solutions

Solutions & Benefits – What works



- Contract with 3 separate suppliers of e-com, in-store and acquiring services
- Contract with an orchestrator to route to an alternative acquirer or PSP
- Consider self-acquiring and in-house processing

A policy adopted by a minority of merchants

Limitations – Potential Problems



- Not in line with modern gateway architectural vision
- Duplication of suppliers – complex to manage failure responsibility
- Each supplier has lower volumes so higher costs
- Complexity of reconciliation and settlement
- Multi supplier implementations and higher risk
- In-house acquiring increases costs of compliance plus scheme membership fees

Difficult to argue case for a multi supplier architecture given higher costs

Option 2 – Cash as a Fallback in Event of Major Outage

Cash as a Fallback

Solutions & Benefits – What works



- Available to all consumers
- Two €50 notes in wallet sufficient!
- Assumes a mandate to continue to accept cash
- In-store ATMs can supply cash
- No liability shift implications
- No submission time limit – low need for electricity
- No authorisations, security, clearing settlement

Simple traditional solution and relatively easy to implement

Limitations – Potential Problems



- Consumer antipathy to carrying cash
- Merchants limited notes/coin float
- Insufficient back-office staff to process
- Limited CIT services for cash delivery / collection
- ATMs unable to handle withdrawal volume
- Would not work for transport and other critical vertical sectors
- Handwritten receipts in event of EPOS/PED failure

Most large merchants have reduced cash handling capabilities, so extra investment needed

Option 3 – Use of EMV Fallback in PED

EMV Fallback

Solutions & Benefits – What works



- Available in all PEDs as standard
- Offline storage of 250 transactions
- Auto submission at end of day option
- Will work with terminal floor limits
- Uses offline chip rules for DDA/CDA set by issuer
- Payments guaranteed solution for settlement
- Uses offline PIN for cardholder verification
- Seamless operation for intermittent down time events

Uses standard EMV fallback processes implemented across EU

Limitations – Potential Problems



- Potential declined transactions – as a result of late batch submission
- Merchant on risk if above floor limit
- Volume limitations – need to detank
- Transactions locked in PED if hardware failure
If no network or WiFi unable to submit
- Complexity of end of day reconciliation
- Potential for fraud and increased chargebacks

If multiple downtime events can be complex to manage

Option 4 – Offline PED and In-store Fallbacks

Offline PED / Server Fallbacks

Solutions & Benefits – What works



- PED enabled to switch route to fallback gateway/acquirer
- PED connected to store server for batch submission
- EPOS/PED as a freestanding unit with dial in end of day
- EPOS/PED operates as a mobile device

Not used widely and considered legacy, but being revisited

Limitations – Potential Problems



- PED a switch – need for tailored payments applications
- Similarly store server software need tailoring
- Dial in – legacy concept to support EPOS
- EPOS/PED as a mobile requires specialised software
- Need for battery driven rechargeable EPOS/PEDs – increased cost
- Two acquirers - so more complex to reconcile and settle

Feasible but complex and costly to implement – terminal suppliers need to adapt!

Option 5 – Central Bank Debit Card / Offline Chip Electronic Money

CBDC Offline Cards

Solutions & Benefits – What works



- Similar concept to Mondex and early stored value cards
- Alternative Payment Method – bypasses domestic/international card schemes
- Assumes CBDC money loaded onto chip-PED operates offline and CBDC value is transferred to merchant
- Merchant deposits CBDC value into own CBDC Account
- Very low cost to merchant – no MSC, scheme fees, interchange

Included within ECB's CBDC deliverables due for implementation in 2027/2028

Limitations – Potential Problems



- Novel and relatively untested concept
- New development required to enable chip loading and merchant transfer
- Concerns over consumer understanding
- Does not generate revenues for acquirers or issuers
- Merchant obliged to have CBDC account

A step back in time – 1980's idea eventually displaced by prepaid cards

Summary of Conclusions

A key large merchant issue is how end-to-end e-comm/in-store acquirers such as Adyen and Stripe deliver a resilient new payments architecture.

1

Multiple Supplier Solutions

Multi supplier complexities with higher costs as lower volumes

2

Cash as a Fallback

A logical solution but consumers must carry. Critical merchants must continue to accept. ATMs and CITs continue to operate – underused assets and high overheads

3

EMV Fallback

Current standard step in – must be a mandated facility. Works well for intermittent outages but not suitable for several days' downtime

4

Offline PED / Server Fallbacks

Solutions workable but more expensive to build and operate. A step back to the 1980/90's

5

CBDC Offline Cards

Novel solution but complex and costly to implement

