Sent by email:

Date: 14 November 2018

The Rt Hon. Nicky Morgan MP
Chair of the Treasury Committee
House of Commons
London
SW1A 0AA

Dear Chair

Following up on our letter to you on 15 June, please find enclosed our summary of EY’s findings from its independent review of the partial service disruption of Visa Europe’s authorization system (VEAS) on 1 June, including Visa’s Europe’s efforts to address EY’s findings.

As detailed in our previous letter, on Friday, 1 June, our European authorisation system was disrupted such that many UK consumers were unable to complete transactions using their Visa debit and credit cards. Notwithstanding the extremely rare nature of the failure, the fact remains that we failed to meet the Committee’s expectations and the expectations of our various stakeholders. As Visa Inc.’s global Chief Executive Officer publicly recognised that day, we also fell short of our own goal of ensuring that Visa payments work reliably 24 hours a day, 365 days a year.

In June, we shared with the Committee that our strategic approach for preventing this type of incident from happening again involved migrating our European processing activities onto our global processing system, called VisaNet. We are pleased to confirm that we successfully completed the migration process in September, without any problems, and the European system has now been decommissioned.

As we described in our 15 June letter, VisaNet is based on a different, and even more robust and resilient, technical architecture than the European system. VisaNet has four active-active images that work in tandem, multiple fallback routes and has significantly more capacity and scale compared to the former European system. VisaNet would be able to isolate and exclude a partially failing switch (like the one that led to the VEAS disruption in June) in a matter of minutes, with virtually no impact to merchants and consumers. In addition to being more resilient overall, VisaNet has also experienced remarkably consistent reliability; more than
99.9995% of transactions were processed properly over the last several years (over a total volume of 319 billion transactions).

Shortly after 1 June, we engaged an external party, EY, to conduct an independent review of the incident. Specifically, EY was asked to perform a root cause analysis, review the factors leading up to the disruption and assess the effectiveness of Visa’s disaster recovery, incident response and communications efforts. The terms of reference were reviewed by the Bank of England and the Payment Systems Regulator (PSR) and are attached to this letter as Annex B.

EY has now concluded its assessment and provided the formal report on 5 October. Our summary of EY’s findings and recommendations and Visa Europe’s efforts to address those findings are contained in Annex A. The Bank of England and the PSR have been closely involved in the development of EY’s report and now have its findings and recommendations. As we work to diligently address these, we will ensure that our regulators continue to have a transparent view of our activities.

Visa Europe has accepted all of the recommendations in the EY report, in full, and is committed to implementing them in a timely manner. Furthermore, the Visa Europe Board is also fully engaged in the delivery of the recommendations that will be reported via our risk committee, with all completed actions subject to further risk review.

As you will see from the summary in Annex A, we note that the findings and recommendations include feedback on how we must improve our internal incident management processes, including more focus on manual response and recovery procedures, improvement of crisis management and communications protocols and enhancement of business continuity measures. As further detailed in Annex A, we have already begun taking important steps to reinforce the resiliency of our systems and implement the other recommendations contained in the report. We have closed out actions on some of the findings already and are making significant progress against those which remain. For example, we have completed the migration of our European processing systems to VisaNet (which already has the additional capabilities that EY recommends for the now decommissioned European system) and are enhancing our global crisis management and communications protocols (with several improvements already made).

In addition, we hope that the learnings from this incident can benefit the larger UK payments ecosystem. To that end, we have also begun efforts to collaborate with our financial institution partners to identify opportunities to work together and further mitigate potential disruptions.

We fully appreciate the very important role we play in upholding the stability of the UK financial system. Our ability to manage, respond to and recover from incidents must not only meet the expectations laid out in the report, but exceed them – and we will not rest until that is the case.

We are grateful for the opportunity to engage with the Committee on this matter. Being able to serve the UK payments ecosystem is a privilege. You have our unequivocal commitment that we will work tirelessly every day to live up to the obligations of that privilege. While the 1 June
incident resulted from a very rare partial switch failure, the lessons to be drawn can be applied broadly across a variety of potential systems scenarios, and we embrace our leadership role working closely with policymakers, regulators, industry participants and other stakeholders, in our increasingly digital and technology-driven world.

Sincerely,

Charlotte Hogg
Chief Executive Officer
Visa Europe

cc John Glen, MP, Economic Secretary to the Treasury
Charles Roxburgh, Second Permanent Secretary to the Treasury
Sir Jon Cunliffe, Deputy Governor for Financial Stability
Andrew Bailey, Chief Executive, FCA
Hannah Nixon, Managing Director, Payment System Regulator
ANNEX A

The assessment was performed using the Terms of Reference as scope (Annex B), with each area assessed against EY’s own resilience framework and industry good practice. This Annex is our summary, for which we take responsibility, of EY’s findings and recommendations provided in the formal report of 5 October, and Visa Europe’s efforts to address those findings and recommendations.¹

It is important to note that the scope and terms of reference for the independent review did not include a requirement for any assessment of the Visa response to the findings. As set out below, we will be completing our own assurance processes around this response. Furthermore, the Visa Europe Board is also fully engaged in the delivery of the recommendations that will be reported via our risk committee, with all completed actions subject to further risk review.

The findings, recommendations and Visa Europe’s response are as follows:

**Finding 1:** Visa Europe has developed a robust and resilient VEAS technical environment intended to prevent a technology outage impacting authorisations

Visa Europe recognises the need for VEAS to be continuously available. This is reflected in key targets set for the service which can be summarised as achieving ‘zero downtime’.

This approach has resulted in a strong track record for availability (100% for 10 years) and quality of processing for VEAS (average transaction quality of 99.999% over 5 years) with no outages since April 2007.

Further, Visa Europe has designed and maintained the service to help ensure that no processing can be lost and that the platform should be always available. Visa Europe’s objective is to deliver to these targets through implementing measures that are aimed at preventing a technology disruption from occurring.

Key steps taken to build resilience and redundancy into the design of the technology environment, include:

- Incorporating two data centres into the underlying infrastructure that supports VEAS which are permanently in Active: Active mode with layers of redundancy for key components, including network switches. This means that each data centre can support running the VEAS application on its own. This design enables the authorisation process to continue should one of the data centres become unavailable.

- Automated response and recovery procedures to take action, when necessary. Visa Europe has modelled a wide range of potential error scenarios such as failure of hardware (including full failure of network switches), or power outage at a data centre, and built redundancy into physical devices and/or software procedures to enable adverse scenario handling for such scenarios to be managed automatically.

- Periodic assessments of future potential increases in transaction volumes to help ensure that VEAS has sufficient capacity

- Only using technology that has a track record to indicate that it can be trusted and relied upon, potentially by having been used in the market for a number of years with no significant issues identified.

¹ EY concluded its fieldwork on 27 June 2018
• Performing regular infrastructure reviews to help ensure that components (both hardware and software) are not approaching their “end of life” which could potentially be affected by the support available in the future.

• Seeking enhanced support from manufacturers to help ensure that Visa Europe has up-to-date manufacturer guidance, including the switch manufacturer.

The technical cause of the VEAS incident on 1st June 2018, as outlined previously, was due to the partial failure of a switch. Typically switch failures mean that the switch ceases to operate, a scenario that Visa Europe had planned for. A faulty or fluctuating switch which has partially failed behaves in an unpredictable manner. Partial failures within data centres, while rare, are considered by the industry as challenging to manage.

Based on the information confirmed by the component manufacturer, the partial failure is an extremely rare event, with no record of exactly the same partial failure occurring despite more than 82,000 switches of the same model currently being used globally.

Against requirements for high resilience, EY believes that management took reasonable steps to architect, build and operate a resilient VEAS technology environment.

---

**VISA EUROPE’S RESPONSE TO FINDING 1**

Visa Europe welcomes this independent confirmation that it had developed a robust and resilient technical environment for the former Visa Europe Authorisation System (VEAS), designed to prevent technology outages that can impact authorisations. In this regard, EY notes VEAS’s strong track record for historical availability (100% over 10 years) and quality of processing (average transaction quality of 99.999% over 5 years).

Our technical environment has been further enhanced by the recent migration of our clients to our global authorisation system, VisaNet, which is now complete. VEAS has now been decommissioned.

Notwithstanding VEAS’s robust technical environment, we are pleased to share that VisaNet has greater capacity and multiple fall back routes than VEAS. VisaNet is also more resilient in its ability to detect and recover even from partial malfunctions of the type that impacted on our European system on 1 June. Overall, VisaNet has experienced consistent reliability: more than 99.9995% of transactions were processed properly over the last several years (over a total volume of 319 billion transactions).
Finding 2: Insufficient preparation of manual technology response and recovery procedures for complex VEAS disruption scenarios

EY’s assessment is that the manual emergency processes applied by technology staff (i.e. to respond to incidents and recover systems should a disruption occur to VEAS outside the scenarios identified) are less mature and have had less focus applied than those established to prevent technology outages from arising.

When reviewing the processes and procedures in place for technology teams to manually respond to and recover from technology disruptions impacting the service, a number of weaknesses were identified:

- IT Disaster Recovery (ITDR) and IT Service Continuity (ITSC) testing have been limited to technical capabilities and automated steps
- Key worst-case scenario “break glass” procedures were not in place
- Site technical recovery plans do not provide thresholds for escalation
- Limited and out of date recovery procedures

Recommendations

EY recommended that Visa Europe:

- Reviews and enhances manual response and recovery capabilities so that if an incident does occur Visa Europe is in a position to respond effectively. This includes enhancing detailed procedures for both plausible and extreme recovery scenarios, reviewing them upon changes to the environment and testing periodically against a broad range of possible and likely scenarios. These procedures should include expected timings of each step and clear procedures for escalation if they are not working.
- Establishes principles for the approach to a range of failure outcomes and possible disruptive scenarios taking into account severe events, such as software and hardware partial failure or degradation. These should include key procedures to be utilised or referenced, escalation protocols and links to break-glass procedures to override standard procedures in crisis situations. Training should be provided to staff on these principles and protocols for escalation.
- Develops and implements further break-glass procedures for overriding standard authorisations during a crisis. Use of these procedures should be tested, where feasible, and monitored to help ensure they are not misused.
VISA EUROPE’S RESPONSE TO FINDING 2

Although VEAS is now decommissioned, a number of steps were completed to enhance its manual response and recovery capabilities between the time of the incident and our completing the migration of all European processing to VisaNet (the migration was paused immediately post-incident). It was important to implement these enhancements to VEAS carefully to balance responsiveness with security. These steps included:

1. Visa Europe developing and installing capabilities that enable isolation and removal of a failing component from the processing environment, allowing the functioning data center to ignore the failing data center and synchronise properly. These “site isolation” procedures were established and tested for scenarios similar to that of the VEAS incident. They also included expected timings for each step identified through testing of the procedures.
2. Visa Europe’s 24x7 operations team were given direct access to the system components, without needing to use the network.
3. As part of the migration to the global systems these processes will be reviewed annually as part of an IT disaster recovery exercise.

As mentioned above, the migration to VisaNet is now complete, materially improving recovery capabilities for our European clients. This includes the capabilities described above, which were already in place on VisaNet.

To ensure that we are able to continue to take advantage of the learnings from this review, we are now in the process of assessing our global systems against them. For example, stress scenarios have been assessed as part of a dedicated resiliency review of VisaNet, and recovery procedures will be updated and tested in line with the results of this exercise. Break glass procedures for gaining access to the data hall have also been implemented as part of the site isolation procedures referred to above. The design and effectiveness of these procedures have also been tested.

Finding 3: Limitations in the effectiveness of crisis management on 1st June 2018 and in the following days

Over the past 12 months Visa Europe has aligned with Visa Inc.’s global incident and crisis management framework. Whilst tests were performed to integrate Visa Europe into the global process, this incident was the first time that a crisis was initiated for a technology and/or business process disruption since the integration.

The feedback from Visa Europe stakeholders was that the internal organisation of the response to the incident was robust and effective. However, as the Crisis Management Team (CMT) did not stand down until 26th July 2018 a formal self-assessment facilitated by global Crisis Management had not yet been conducted at the conclusion of our fieldwork.

EY’s analysis of Crisis Management plans and artefacts from the incident, as well as interviews with those taking part in the response at various levels, identified a number of areas for improvement relating to the Tactical Response Team (TRT) and CMT during the incident, including:

- **Crisis management protocols delayed escalation and communications**: The crisis management framework does not provide guidance when escalation directly to a full CMT would be appropriate (i.e. in obvious crises).
• Definition of roles and responsibilities on the CMT

• Social media was not proactively monitored during the incident

EY’s analysis of Visa Europe’s response to the incident in the days that followed 1st June 2018 identified the following findings:

• **Plans for sharing information on the impact of incidents to processing were not clear prior to or following the incident**: Visa Europe did not have plans prepared to be able to share data with their clients to help them assess the impact of the incident on their customers.

• **Client redress approach was not formalised**

EY was informed by management that a number of actions are planned internally to resolve issues identified in the incident response and crisis management process. These are expected to be captured in the Crisis Management self-assessment process, which this report will form an input to.

**Recommendations**

EY recommended that Visa Europe:

• **Reviews Crisis Management protocols and plans to implement improvements identified through this review including refreshed escalation protocols and roles and responsibilities, separating the Incident Commander from subject matter, or providing a role for an incident manager delegate. Any changes to protocols should be robustly tested with key internal and external stakeholders.**

• **Reviews Crisis Management and scenario plans to include principles and protocols for providing information to relevant stakeholders to help them better understand, respond to and recover from incidents.**

• **Reviews and enhances the monitoring of channels such as social media to better understand incidents.**

• **Reviews and enhances incident and scenario playbooks to ensure that other stakeholders’ requirements such as impact data and consideration of ex-gratia redress are considered where relevant.**
**VISA EUROPE’S RESPONSE TO FINDING 3**

- Global Crisis management protocols and plans are being reassessed through a phased approach (to be agreed internally by Nov-30 2018, and implemented throughout FY19). In particular:
  
  o We have reassessed the leadership representation to ensure appropriate decision makers are part of the crisis management response. We are also enhancing the crisis management responsibilities to further ensure that there is clear understanding of the role of an Incident Commander and separating this from the subject matter experts and identified alternatives. We are reviewing the crisis management escalation triggers, and have engaged external consultants to assist us with these changes.
  
  o We plan to complete an exercise on the Incident Commander, related delegate roles and leadership representation, as well as the updated escalation triggers, as part of Crisis Management's annual programme cycle for core services.

- We have reviewed and updated our crisis communications procedures which now include more detailed guidance and enhanced processes for notifying stakeholders in the event of an incident. For example, during the remaining migrations to VisaNet this included establishing call bridges and enhanced senior leadership oversight where significant clients were migrating. These were in place immediately after the VEAS incident. Next steps include discussions with key stakeholders to ensure their specific requirements are identified and incorporated into our procedures as appropriate.

- Additionally, a simulation of the updated communication protocol is to be performed with key issuers and acquirers in early November 2018.

- We have also implemented our enhanced social media monitoring tool since the VEAS incident. Monitoring is performed by Visa Europe’s 24x7 operations team and escalated to Corporate Communications in the event that relevant, defined thresholds are exceeded. The thresholds are defined by the volume of “tweets” within a short time period that meet a set of pre-defined keywords, such as declines or denials, in multiple European languages.

- Finally, the Client Incident Playbook is in the process of being updated to reflect the outcome of the review referenced above. This will also include “impact analysis” templates. Visa’s Core Rules already set out the liability principles that apply in relation to system errors.
Finding 4: Insufficient preparation to deliver Authorisations business process continuity and quality through a disruption

EY’s review has identified that when a disruption did occur, Visa Europe was insufficiently prepared in terms of authorisation business process response, recovery and continuity capabilities. As an illustrative example, the draft Visa Client Incident Playbook – Europe, sets out a number of crisis scenarios that could impact the Clearing and Settlement service, and the business workarounds identified. However, the playbook does not identify business workarounds for Authorisations, instead stating that Visa Europe will “work to remediate the issue”.

Operational resilience is defined as the ability of an organisation and the sector as a whole to prevent, respond to, recover and learn from operational disruption. As the Bank of England, FCA and PRA joint Discussion Paper released in July on “Building the UK financial sector’s operational resilience” (DP1/18) states:

“Avoiding disruption to a particular system supporting a business service is a contributing factor to operational resilience. But ultimately it is the business service that needs to be resilient – and needs to continue to be provided. The supervisory authorities envisage that boards and senior management should assume that individual systems and processes that support business services will be disrupted, and increase the focus on back-up plans, responses and recovery options.”

Continuity and recovery procedures and protocols, are a key component of effective operational resilience in minimising the impact of an incident on users of the authorisations service.

Recommendations

EY recommended that Visa Europe:

• Reviews, develops and tests continuity arrangements for the authorisations business process. Given the migration to the global authorisations platform, a refreshed approach may include components such as:

  o Risk assessment to determine the nature of authorisation business process continuity arrangements required.
  o Expected benefits.
  o Pre-prepared liability and authorisation protocols for different scenarios.
  o Functional testing requirements.
  o Test steps to invoke continuity arrangements.
  o Scenario-based testing with key parties to ensure that both the processes for initiation and the broader implications for the ecosystem are understood and prepared for.

• Considers the communication plans and protocols that will be required to enable effective continuity arrangements and information sharing between participants in the ecosystem. These need to consider which parties need to know what, and when. The protocols should be proactively communicated to, and tested with, key stakeholders.

• Assesses why Visa Europe failed to maintain operationally effective business process continuity and recovery arrangements for significant disruptions to the authorisations

2 Bank of England DP01/18; Prudential Regulation Authority (PRA) DP01/18; Financial Conduct Authority (FCA) DP18/04 “Building the UK financial sector’s operational resilience”, Box F: Managing risks in the end-to-end processing of payments; page 24, accessed 24/07/2018
service since these were first designed in 2007. Based on this assessment, identify how lessons learned will be addressed in future approaches.

VISA EUROPE’S RESPONSE TO FINDING 4

In addition to the steps noted above in relation to Finding 3, we also convened a meeting of our UK Client Council on 28 September. The UK Client Council is a regular, independently chaired client engagement meeting that is composed of approximately 20 of Visa Europe’s largest issuing and acquiring clients, representing all our major UK financial institution stakeholders. The session on 28 September 2018 covered the following topics:

- EY’s report and findings;
- Response on a future similar incident;
- Discussion on how ecosystem resilience can be improved including consideration of the joint Bank of England/Prudential Regulatory Authority/Financial Conduct Authority discussion paper on operational resilience (to which Visa has already responded).

Visa Europe has scheduled subsequent working sessions with ecosystem participants to discuss these issues, recommendations arising from them and their implementation. Two workstreams were created after the 28 September UK Client meeting:

- Client Communications - simulation of client communications as part of a crisis management exercise similar to the VEAS incident with top issuers and acquirers. This will be performed in early November.
- Operational resilience – focusing on potential solutions and testing for disrupted parties (e.g. issuers, acquirers and merchants). A project plan is in place with target milestones to be executed over the next six months with external expert guidance. For example, one option we are considering is seeking to establish “Acquirer Stand In” arrangements with certain acquiring clients (which would establish parameters for acquirers to authorise transactions on behalf of Visa).

Recognising the importance of client needs in different markets, we already had in place Client Councils in various European locations prior to the VEAS incident. These Councils aim to increase engagement across different markets in which we operate, and are made up of representatives from our clients.

RESPONSE TO FINDING 4 CONTINUED ON NEXT PAGE
VISA EUROPE’S RESPONSE TO FINDING 4 CONTINUED

As part of our engagement with clients (referred to above), we are working to establish the following:

- Continuity communication protocols when an incident occurs; and
- An agreed frequency and methodology for testing communication methods (noting the need for appropriate coordination with, and cooperation from, clients).

We had initiated discussions with our two largest acquirers in 2007 on arrangements that seek to drive operational resilience in case of a disruption of the Visa Authorization Services. While agreements had been drafted in support of these arrangements, these had not been fully executed / embedded:

- There was no common agreement on accepting liabilities across the partners in the ecosystem.
- We had not been able to fully validate the effectiveness of these arrangements given the operational complexity and its focus on ongoing migration.

We are actively pursuing efforts to strengthen operational resilience across the ecosystem, and will apply lessons from our past efforts into our current approach. We are doing so (a) by identifying and assessing a broader set of solutions that can drive operational resilience; (b) by driving broader/stronger client engagement through active involvement of its UK Client Council and (c) by leveraging the regulatory thinking on operational resilience as defined in the recent Discussion Paper that applies to both Visa and its clients.

Finding 5: Communications with internal and external stakeholders during the incident were not timely, regular or actionable

EY’s assessment of communications considered a range of internal and external stakeholder groups including the Visa Europe Board, Visa Inc. Operating Committee, Regulators, Clients, Cardholders and Merchants. The assessment of communications considered the following key attributes, which are based on industry good practice for crisis communication: timeliness, clarity, regularity, providing information that is actionable, and includes a clear expectation of when stakeholders will receive further updates.

EY’s assessment did not identify findings relating directly to communications with Visa Europe’s Board, or the Visa Inc. Operating Committee, and during interviews with members of the Board, EY was informed that the Board felt adequately informed during the incident.

Dissatisfaction with communications during the incident, was strongly emphasised by the sample of 15 Visa Europe clients interviewed in this review.

EY’s assessment of communications during the incident identified two significant findings:

- **External communications were not timely or regular**
- **External communications were not actionable**

Further communications findings identified by the assessment include:
• Remediation of communications issues identified in previous incident

• Delays in communication approvals

• Internal communications were not timely, actionable or delivered through effective channels

• Methods used to communicate with clients were not effective or efficient

EY that the extent and frequency of communication improved in the days and weeks after the incident.

Recommendations

EY recommended that Visa Europe:

• Reviews and enhances the crisis communication strategy and response plans to support more timely, regular and insightful communication to stakeholders. This should be supported by putting in place the processes and tools to support the execution of crisis communications and to ensure these are tested on a regular basis.

• Considers its approach to, mechanisms and tools for internal communication during a crisis to improve the sharing of information to external-facing staff.

• Assesses why it failed to finalise, socialise and implement the Client Incident Playbook committed to following a significant incident in 2017. Based on this assessment, identify how lessons learned will be addressed in future approaches.

INTENTIONALLY LEFT BLANK
VISA EUROPE’S RESPONSE TO FINDING 5

- We are committed to enhancing crisis communications. We have initiated a project in consultation with clients to further co-ordinate incident communications. We are updating playbooks to include:
  - Communication approval process: (i) improving the process for more timely approval by key stakeholders across Europe and sequencing with Global Communications; (ii) establishing closer coordination across regulatory and client facing teams and other functions. The European Crisis Communications Playbook has been updated accordingly.
  - Frequency of updates: Based on the profile of an incident, identifying opportunities to enhance frequency, and up to date channels of communication with relevant stakeholders (for example, in the immediate days after the incident (2 – 19 June), Visa sent 11 further updates to clients).

- In addition to this, we are also assessing the feasibility of rolling out our “v-alert” messages to clients as an immediate information sharing mechanism during an incident.

- In response to the significant incident in 2017, we created a Client Incident Playbook that was socialized internally and at the UK Client Council meeting in Q1 2018. Further updates were made throughout the year but the document was not fully implemented.

- To ensure we fully execute on the actions of this plan, we have established an Oversight Committee that is chaired by the Chief of Staff to the CEO. The Committee will meet regularly to discuss progress on actions and help resolve any roadblocks.

- All completed actions will be subject to a 2nd line Risk review that will assess the effectiveness of the remediation.

- Progress reports from the Oversight Committee and the Risk Reviews will be reported to our Europe Risk Committee. Where required, any exceptions to achieving remediation will be subject to formal risk acceptance.
Observation 1: Consider lessons learned from the incident relating to Visa Europe’s role in maintaining the resilience of the payment processing “ecosystem”

Visa Europe’s service is considered systemically important in the UK and disruption could have a potentially significant impact on other European economies where Visa Europe processes a significant share of debit transactions.

Visa Europe recognises legal responsibility to clients, but also broader obligations to Cardholders and Merchants to provide a resilient service. Whilst Visa Europe does not have a direct contractual relationship with Cardholders, or Merchants, it is a key supplier to Financial Institutions that rely on Authorisation and Settlement services to provide payments services to their customers (whether consumers or Merchants).

EY’s assessment is that Visa Europe has clearly defined its legal duties for clients, but further focus is required to clarify and codify response, recovery and communication procedures taking into account Cardholders, Merchants and other participants in the Visa Europe ecosystem. The findings that support this assessment are included in 4.3, 4.4 and 4.5 above.

In interviews with Visa Europe, Acquirers and Issuers, many referred to disaster recovery and incident response procedures that are developed within their own organisation. However, there has been no formal end-to-end scenario planning involving representatives of the broader payments ecosystem (i.e. different payments systems and their respective users / providers). Such exercises have been conducted in recent years to consider the impact, complications and likely responses to a disruption to cash distribution services in the UK market, with many firms finding these a useful exercise.

End-to-end scenario planning is complex, and is not in the control of Visa Europe alone. Visa Europe has acknowledged that a greater degree of collaborative planning would be in the interests of the ecosystem as a whole as stated in their response to the Treasury Select Committee (TSC):

“[Visa have] initiated detailed discussions with our financial institution partners about how to improve the operational resilience of the ecosystem based on this specific incident. To ensure a seamless payments experience for consumers and merchants alike, we are looking at options that might mitigate the potential of any impacts in the future, including ecosystem scenario planning.”

As focus on operational resilience increases within financial services, EY concurs that there is a need for increased end-to-end scenario planning and testing, and support Visa Europe’s commitment to drive improvement in this area.

This is in line with the July 2018 Discussion Paper “Building the UK financial sector’s operational resilience”, published jointly by the Bank of England, FCA and PRA after (but not as a direct result of) the incident which notes:

“Individual firms and FMI’s <Financial Market Infrastructure> are responsible for their own robustness and security. However, it is important that participants work together to deliver the resilience of the end-to-end processing of payments within the network.
This is a good example of how an FMI can work together with its participants and other stakeholders to mitigate risks to financial stability.”

3 Bank of England DP01/18, Prudential Regulation Authority (PRA) DP01/18; Financial Conduct Authority (FCA) DP18/04 “Building the UK financial sector’s operational resilience”, Box F: Managing risks in the end-to-end processing of payments; page 24, accessed 24/07/2018

Annex A: Page 12 of 15
It is EY’s view that the incident of 1st June 2018 could stimulate significant improvements in the planning for resilience of the payments ecosystem. Visa Europe, leading Issuers and Acquirers will need to invest time and energy to tackle resilience challenges in partnership, as no individual firm has the authority or capability to effect the change required unilaterally.

Recommendations

EY supports Visa Europe’s commitment to drive improvement in this area and recommends that it:
• Leverages its influential role in the broader payments ecosystem, championing collaboration and encouraging improvements in the operational resilience of this ecosystem.

VISA EUROPE’S RESPONSE TO OBSERVATION 1

During the 28 September client meeting, Visa Europe raised the issue of conducting a broader ecosystem crisis management exercise, which resulted in the creation of two workstreams (see response to 4 above). This will include identification and assessment of the feasibility of various potential operational solutions to improve ecosystem resilience, developed in collaboration with our issuer and acquirer clients and other participants.
Observation 2: Consider the impact of this incident in the context of the VEAS to VisaNet migration

The migration of Visa Europe clients to the Visa Inc. authorisations platform, VisaNet, is a significant change in the operation of the authorisations service. The migration programme is outside the scope of EY’s review.

Recommendations

EY recommends that the following points are considered by Visa Europe in maintaining authorisations resilience when systems have migrated to VisaNet:

- Assesses whether the approach to preventing, responding and recovering from technology disruptions of the VisaNet service is equivalent or exceeds that of VEAS. Take into account the findings identified above and consider whether they need to be read across to VisaNet.

- Assesses any changes required to incident response protocols to reflect the changing roles and responsibilities of stakeholders in Visa Europe and Visa Inc.

- Assesses any changes required to communication roles, responsibilities and protocols, including requirements for approvals, in the context of Visa Europe relying on Visa Inc. services. Whilst the framework for global crisis management and communications may be common, Visa Europe should understand and test for the differences in the European market and needs of key external stakeholders.

- Continues to review contingency arrangements for authorisations, in the context of the VisaNet migration to help ensure that when disruption occurs a robust fall-back option is available.
VISA EUROPE'S RESPONSE TO OBSERVATION 2

VisaNet is based on a different technical architecture from the European system (VEAS), has multiple data centres, and serves multiple geographies. VisaNet has four active-active images that work in tandem, and has significantly more capacity and scale compared to the European system.

VisaNet is more resilient in its ability to detect and recover from partial malfunctions of the type that impacted our European VEAS system on 1 June. It can isolate and exclude a failing (including a partially failed) component with one command, taking no more than a few minutes to exclude the malfunctioning component from the processing environment. Therefore, in the case of the 1 June incident, VisaNet would have been able to re-route the impacted transactions within minutes. Based on our experience, this will deliver greater system redundancy, resilience and processing capability to all of our stakeholders in Europe now that Visa Europe has fully migrated to the VisaNet platform. Nonetheless, we are committed to performing our ongoing technology review of VisaNet resilience, and have assessed “what-if” scenarios for VisaNet resilience (taking into account the findings in the EY report regarding the VEAS incident where relevant).

A review of Visa’s global incident response and crisis management processes is underway, and are following up with regard to specific European requirements, as well as regarding Visa Europe’s interaction with European clients and other relevant stakeholders in the event of an incident, to ensure that these are appropriately reflected in the review.

Please also refer to our responses above.

As detailed above, Visa Europe has accepted all of the recommendations in the EY report in full. We have already begun taking important steps to reinforce the resiliency of our systems are committed to implementing the other recommendations contained in the report.

The Bank of England and the PSR have been closely involved in the development of EY report and now have its findings. As we work to diligently address EY’s findings, we will ensure that our regulators continue to have a transparent view into our efforts.
ANNEX B

The following are the key areas of scope and objectives of the review.

- **Review the Root Cause Analysis ("RCA")**
  Review of the effectiveness and thoroughness of the root cause analysis performed to date, as well as action items captured for remediation and prevention of recurrence.

- **Evaluate the leading factors of the Incident**
  Independent assessment of the leading factors that contributed to the Incident. This includes consideration of system and architecture design, ongoing system and hardware maintenance and support, impact of system or organisation changes, lessons from prior incidents, formal risk mitigation, capacity management, and testing.

- **Review the effectiveness of VEL’s disaster recovery**
  Assessment of disaster recovery procedures and the readiness of VEL to effectively execute them on a timely basis. This includes consideration of the breadth of incident scenarios; the awareness of those involved of their roles and responsibilities; the procedures needed to be initiated outside of VEL (e.g. by Acquirers); and the extent of testing performed.

- **Review the effectiveness of VEL’s response to the incident**
  Review of the chronology and effectiveness of VEL’s response to the Incident. Including consideration of roles and responsibilities, escalation procedures, resource availability, stakeholder engagement (internal and external).

- **Review the effectiveness of VEL’s communication with stakeholders**
  Assessment of VEL’s communications related to the Incident. Including consideration of communication with internal and external (e.g. clients, cardholders, merchants, and relevant regulators) stakeholders.

Notes on the summary of the EY report:

a) EY issued a formal report on 5 October 2018 (on the basis of fieldwork which was concluded on 27 June 2018) and this report was provided in full to Visa Europe, the Payment System Regulator and the Bank of England;

b) The summary provided to the TSC has been prepared by Visa Europe, who takes full responsibility for its contents; and

c) The summary being provided has not been reviewed, or approved, by EY.