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

15 June 2018  

Dear Chair,

Thank you for your letter dated 4 June 2018 regarding the partial service disruption that prevented many cardholders from using Visa’s European systems for payments on Friday 1 June. We appreciate the opportunity to address this important issue in detail, including our response to your questions below. We do absolutely hold ourselves accountable to the consumers and merchants who use our cards. In this instance, we failed to meet your and our own expectations, and we apologise again unreservedly to everyone who was affected by the incident. Visa, together with our financial institution partners, has quickly implemented a compensation programme for cardholders in response.

The integrity of payment systems is vitally important to the UK economy and, to this end, we are regulated by the Bank of England and the Payment Systems Regulator. Visa holds itself to the highest standards with respect to the performance of our systems, and we aim to exceed the expectations of cardholders, merchants, financial institutions and other stakeholders. We also understand the role of our system in supporting commerce throughout Europe. As Visa Inc.’s global Chief Executive Officer recognised publicly on the day of the incident, we fell short of our goal of ensuring that Visa payments work reliably 24 hours a day, 365 days a year.

In this letter, we aim to provide you with full and complete responses to your questions. We focus on what occurred, how we mitigated and are continuing to mitigate potential impacts to consumers and other stakeholders, and what we are doing to prevent any reoccurrence or similar incident. We first summarise the incident below, and then address the questions of the Committee.

On Friday 1 June, our UK processing systems were disrupted such that many UK consumers were unable to complete transactions using their Visa debit and credit cards. The incident began at 14:35 British Summer Time and ended at 00:45. At its peak, the disruption affected people in the midst of returning home from work, socialising in restaurants and pubs, and doing end-of-day shopping. We take seriously our important role in supporting financial stability in the UK. A disruption to our processing that impacts consumers at any time is unacceptable, let alone during a busy Friday afternoon.
To assist the Committee in understanding fully the incident, we think it would be helpful to provide further detail on Visa’s role in the payments ecosystem. Visa connects the financial institutions that issue cards to their customers (issuers) with other financial companies who ensure that merchants are able to safely connect to the network (acquirers). We have provided detail on Visa’s role in the payment ecosystem in an appendix.

**The Incident and Visa’s Response**

At 14:35 on Friday 1 June, our UK data centre operations team became aware of a partial degradation in our processing system. We immediately took steps at our data centres to attempt to remedy the issue and initiated a response based on protocols we have in place for addressing any type of critical incident; the first step was a Technical Response Team assessment meeting. Soon thereafter, we escalated the matter in alignment with our crisis management protocol. Ninety minutes after our first indication of a systems issue, and having confirmed the underlying facts as part of our crisis management protocols, we provided a public statement to the media.

Our number one priority was to focus our resources on identifying the root cause and implementing a variety of solutions to get the system back to full capacity. By way of background, we operate two redundant data centres in the UK, meaning that either one can independently handle 100 percent of the transactions for Visa in Europe. In normal circumstances, the systems are synchronised, and either centre can take over from the other immediately. The centres communicate with each other through messages regarding the system status, in order to remain synchronised. Each centre has built into it multiple forms of backup in equipment and controls. Specifically relevant to this incident, each data centre includes two core switches (a piece of hardware that directs transactions for processing) – a primary switch and a secondary switch. If the primary switch fails, in normal operation the backup switch would take over.

In this instance, a component within a switch in our primary data centre suffered a very rare partial failure which prevented the backup switch from activating. As a result, it took far longer than it normally would to isolate the system at the primary data centre; in the interim, the malfunctioning system at the primary data centre continued to try to synchronise messages with the secondary site. This created a backlog of messages at the secondary data centre, which, in turn, slowed down that site’s ability to process incoming transactions.

Due to this complexity and the very rare partial failure of the switch, a number of key steps were taken throughout the afternoon – including turning off software applications at the primary site and cleaning up message backlogs at the secondary site by both manual and automatic means. It took until approximately 19:10 to fully deactivate the system causing the transaction failures at the primary data centre. By that time, the secondary data centre had begun processing almost all transactions normally. The impact was largely resolved by 20:15, and we were processing at normal service levels in both data centres by Saturday morning at 00:45, and have been since that time.
The service disruption lasted from 14:35 to 00:45. This length of time was clearly unacceptable. However, at no time during the incident was there a full system outage. Instead, throughout the period of disruption, the percentage of transactions that failed to process fluctuated. Over the course of the entire incident, 91 percent of the transactions of UK cardholders processed normally; approximately 9 percent of those transactions failed to process on the cardholder’s first attempt. There were two periods of peak disruption: the first for ten minutes (15:05-15:15), the second for 50 minutes (17:40-18:30), during which an average of 35 percent of transactions failed to process for UK cardholders. Over the remainder of the incident (excluding the peak periods), the rate of failed transactions in the UK was closer to 7 percent on average.

Our analysis of the data shows that many cardholders retried the same transaction at least once during the incident. When this is taken into account, the 9 percent rate of transactions that failed to process properly over the entire incident window for UK cardholders falls by approximately half.

For clarity, we use the term “failed to process” to refer to two circumstances: either when Visa’s system did not respond within required time limits (generally 10-15 seconds) so the transaction “timed out”, or the transaction was improperly declined due to a Visa system error. It is important to note that, at any time, some cardholders may experience a declined card as a result of fraud and risk monitoring tools, incorrect information such as an expired card, or insufficient funds to complete the transaction.

Given that consumers may have access to another payment brand’s credit or debit card, cash, or Faster Payments, many more purchases are likely to have been completed. For context, we estimate that 40 percent of debit cardholders in the UK also carry a credit card from MasterCard or American Express. Regardless, we fully realise the level of frustration and inconvenience created for our cardholders. We provide further detailed data on the impact of the incident in responses to your questions below.

Since the system was fully restored, our priority has been to address and limit any remaining impact for cardholders, and to proactively put in place mitigating steps for merchants, working with our financial institution partners. Since 1 June, we have also been focused on identifying all necessary steps to prevent a reoccurrence and ensure that Visa’s incident response is enhanced in the future by applying any lessons learned. We are undertaking both a rigorous internal review, and bringing in an independent third party to ensure we fully understand and embrace lessons to be learned from this incident.

The Committee’s Questions

We have provided below answers to the questions in your letter. Where relevant, we have expanded on answers to provide context and further insight. We have also provided additional details in the appendix.
1. **When did Visa first become aware of the failure, and when were you personally informed of it?**
   - Our UK data centre operations team first became aware of a partial degradation of service levels at 14:35 on Friday 1 June, and we immediately undertook efforts to remedy the issue.
   - At 14:45, in line with our protocols, a Technical Response Team was convened, escalating the incident to all relevant European support teams and continuing work on identifying and addressing the issue.
   - The next step-up in our process was to have an assessment call at 15:19, followed by the mobilisation of the full Crisis Management Team at 15:56. I learned about the incident at 15:51, and led a meeting of the Crisis Management Team at 16:00.

2. **For how long were you aware of the system failure before issuing your first public statement on the incident?**
   - Ninety minutes after our first indication of a systems issue, and having confirmed the underlying facts as part of our crisis management protocols, we provided a public statement to the media.
   - We used a pre-prepared plan to produce a statement to inform the public that we were experiencing a technical issue that prevented some consumers from making purchases with Visa cards. Our goal was to minimise confusion among merchants and consumers.
   - This statement said: “Visa is currently experiencing a service disruption. This incident is preventing some Visa transactions in Europe from being processed. We are investigating the cause and working as quickly as possible to resolve the situation.”
   - The initial statement was provided to media at 16:05 and also shared with our client-facing staff to support them in managing enquiries.

3. **How many Visa cards were affected by the system failure, and how many of those were issued in the UK?**
   - We have conducted an analysis of the incident – the below data outlines how many Visa cardholders were impacted by Visa's service disruption in total, and in the UK. The numbers reflect information currently available in Visa systems.
   - Overall, for cards issued both in the UK and elsewhere, during the period of the service disruption, 51.2 million Visa transactions were initiated and sent to Visa's European systems for processing. Of these, 5.2 million (10%) failed to process correctly. Many consumers attempted to make their transaction again following a failed transaction. When we take these retried transactions into account, the rate of transactions that failed to process properly dropped by approximately half.
   - When discussing the impact, we use the term "cards" and "cardholders" to refer to data based on a unique 16-digit account number. We also note that many cardholders may carry more than one Visa card.
   - We focus below on the impacts for UK-issued cards.
Cardholder Accounts -- UK

- During the period of disruption, a total of 16 million cards were used and around 1.7 million were impacted (10.4%).
- As mentioned above, many consumers attempted to make their transaction again following a failed transaction. A large number of these transactions were processed properly. Taking this into account, the number of affected cards falls to approximately 1.1 million (6.7%).

Transactions -- UK

- During the incident window, there were 27.6 million Visa transactions initiated on UK-issued cards and sent to Visa for processing. Of these, 25.2 million transactions were processed properly (91%) and 2.4 million (9%) failed to process.
- As above, it is important to note that, after a transaction did not go through, many merchants and consumers retried their cards to attempt to complete the transaction. Since many of these retried transactions processed properly, taking these into account, the 9 percent overall rate of transactions that failed to process for UK cardholders over the course of the incident then dropped by approximately half.

4. What determined whether or not a given Visa card was affected?

- From an individual cardholder and merchant perspective, the distribution of impact was largely random. Throughout the period of disruption, the rates of decline fluctuated due to the nature of the technical fault in the system.
- As noted, over the course of the incident, 91 percent of the transactions of UK cardholders processed normally, and 9 percent failed to process on the cardholder's first attempt. There were two periods of peak disruption: the first for ten minutes (15:05-15:15), the second for 50 minutes (17:40-18:30), during which an average of 35 percent of transactions failed to process for UK cardholders. Over the remainder of the incident, excluding the periods of peak disruption, the rate of failed transactions for UK cardholders was closer to 7 percent on average.

5. You have stated that the incident was caused by a hardware failure. What led to this hardware failure, and what controls do you have in place to prevent such failures from occurring?

- The incident was caused by the failure of a switch in one of Visa's data centres. To be clear, this was not a cyber-related incident.
- We understand what hardware malfunctioned (the switch), and the nature of the malfunction (a very rare, partial failure). We do not yet understand precisely why the switch failed at the time it did, but we are working with the manufacturer to conduct a forensic analysis of the switch.
- Visa processes payments in Europe in two data centres in the UK. The system works as an "active-active" service so both sites are continually processing transactions.
- The two sites are designed to continuously synchronise with one another, so that if one site encounters issues, transactions are routed to the other for processing. It is important
to note that each data centre has the full capacity to independently handle 100 percent of the transaction processing.

- In this instance, the switch being used in our primary data centre experienced a very rare, partial failure, which impacted the secondary site and prevented it from automatically processing all transactions, as it should have. As a result, it took far longer than expected to isolate the primary site; in the interim, the malfunctioning system at the primary data centre continued to try to synchronise messages with the secondary site. This created a backlog of messages at the secondary data centre, which, in turn, slowed down that site's ability to process incoming transactions.

- Due to the complexity and the very rare partial failure of the switch, a number of key steps were taken throughout the afternoon - including turning off software applications at the primary site and cleaning up message backlogs at the secondary site by manual and automatic means. It took until approximately 19:10 to fully deactivate the system which was causing the transaction failures at the primary data centre. By that time, the secondary site began processing almost all transactions normally. The impact was largely resolved by 20:15, and we were processing at normal service levels in both data centres by Saturday morning at 00:45, and have been since that time.

- We have detailed the steps that we are taking to address this issue resolution time period in the answer to question 10.

6. Some merchants were left unable to accept any card payments, even those taking place over an alternative card network (e.g. MasterCard). Why did a Visa system failure prevent some non-Visa transactions from taking place?

- As a service to our clients, Visa supports the ability of acquirers to send transactions of certain other networks to our European systems; those transactions are typically handed off to those other networks for processing. This service, called a gateway, generally involves a relatively small number of transactions. Analysis to date indicates that fewer than 1000 transactions on this gateway service were impacted.

- Other than this limited gateway service, Visa does not process transactions of other payment schemes (e.g. MasterCard).

- We have raised the question of potential impact on other forms of payment in discussions with many of our clients, including the acquiring financial institutions that work with merchants. We understand that a number of merchants decided temporarily not to accept any cards and move to 'cash only' due to the level of declines they experienced.

7. Does Visa operate a backup processing site? If so, why was processing not switched to this site to ensure service continuity?

- Yes. Visa operates two data centres in the UK. Please see answer 5 above.

- As detailed further above, processing at the secondary site was impacted by a backlog of messages which in turn slowed down that site's ability to process incoming transactions. However, an interconnected series of steps was necessary in order to fully shut off the malfunctioning switch, isolate the primary data centre and stop the backlog of messages, so the secondary site could take over processing all transactions.
8. Have any cardholders seen money leave their accounts for transactions that were not, in fact, completed?

- No. Cardholders should not in any cases be charged for transactions they did not complete.
- Throughout the service disruption and following the incident, Visa worked closely with all of our financial institution clients to support them in managing any issues that have arisen with their customers as a result of this disruption.
- This includes instances where the transaction failed to process, but a "hold" for a pending transaction was placed on the cardholder’s account by the issuer.
- From the outset we have worked with our Visa card issuers across Europe to provide them with the data and support they require to ensure that cardholders have not been charged for transactions they did not complete, and that pending transactions have been resolved and removed from impacted accounts.
- As an example of our ongoing commitment to cardholders, Visa’s zero liability policy protects cardholders against unauthorised or fraudulent charges. Under the terms of this policy, consumers are not held responsible for such charges and will be reimbursed through their card issuing financial institution.

9. Will any cardholders or merchants be entitled to compensation from Visa?

- We take our responsibility to consumers very seriously. Although the issuing banks have the direct customer relationships, Visa wants to ensure that our cardholders are treated properly.
- We are working closely with our issuing banks in the UK to address the impacts of the incident, including appropriate compensation of cardholders. Given that cardholders expect to work with their card-issuing bank on disputes or concerns about use of their cards, Visa has communicated with issuing banks in the UK that it will stand behind redress of those customers by reimbursing issuers for payments they make to cardholders as a result of the incident. The banks are best placed to review these specific circumstances on a case by case basis. This approach is consistent with the advice given by consumer experts, including Which? and Money Saving Expert, which recommend that customers keep receipts and speak to their banks (their issuers) about the incident.
- When it comes to merchants, Visa’s commercial relationship is with financial institutions that offer payment services to merchants – the acquirers. We have been working with our acquirer clients to understand the concerns of their merchant customers.
- Visa is waiving fees to UK acquirers for transactions which failed to process. For our UK acquiring clients and merchants, Visa is also establishing a programme to mitigate processing-related fees they may have incurred through their acquirers as a result of transactions that failed to process.
- In response to the incident, Visa is also conducting a survey of small merchants to solicit their input and better understand their core business needs and identify specific tools to help them grow their businesses.
10. What steps will you be taking to ensure a similar system failure does not happen again?

We are focusing on the following five actions to ensure that we avoid a similar incident in the future.

I. Technical steps

- We removed components of the switch that malfunctioned and replaced them with new components provided to us by the manufacturer. We are currently working with the manufacturer to conduct a detailed forensic analysis of the switch. Based on their initial findings, we have been informed this was a very rare failure.
- The manufacturer has provided us with recommendations on software for automating the monitoring and shutdown of the switch in the event of a similar type of malfunction. When operational, the programme will continuously review key components in the switch to track their availability. If the same errors are detected, the programme will automatically take the component or switch out of operation.
- We are working internally to develop and install other new capabilities that would allow us to isolate and remove a failing component from the processing environment in a more automated and timely manner.

II. Operational steps

- As discussed above, we managed the failure of the switch utilising established operational protocols for responding to any type of significant incident in a timely, effective manner. That said, we are carrying out a wide review and testing of our operational and incident response processes, and we will apply the lessons learned from this review.
  - We are also enhancing our incident response plans so that the teams on the ground are fully prepared to handle this type of scenario using the new technical capabilities described above.
  - Moreover, we are changing our crisis management protocols to ensure that we prioritise communications to all relevant stakeholders.
- We are performing a wide review of other failure scenarios, and testing our responses, so that our teams are always prepared to respond to an event, no matter how rare or exceptional.

III. Expanding global systems to Europe

- Our strategic approach for preventing this issue from happening again is migrating our European processing onto our global processing system called VisaNet. This migration is planned to be completed by year-end. VisaNet is based on a different technical architecture from the European system, 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 system on 1 June. It can isolate and remove a failing component with one command, taking mere minutes to remove the malfunctioning
component from the processing environment. By doing so, our operating systems at other
data centres can ignore a malfunctioning system and continue to operate seamlessly.

- Based on our experience, this will deliver greater system redundancy, resilience and
  processing capacity to all of our stakeholders in Europe. For example, VisaNet has
  experienced consistent reliability; more than 99.9995% transactions were processed
  properly over the last several years (over a total volume of 319 billion transactions).
- It is worth noting that the incident on 1 June was in no way related to this migration, which
  has been underway since February and has been going well, following a robust migration
  plan. As we progress, we are putting additional steps and governance into the migration,
  and working with our clients to incorporate lessons learned from this incident.

IV. External review

We have also engaged an external party, EY, to conduct an independent review of agreed
aspects of the incident. The Terms of Reference have been reviewed by our UK regulators.
This will include:
  o Review of the root-cause analysis
  o Evaluation of the leading factors in the incident
  o Review of the effectiveness of Visa Europe’s disaster recovery, its response to the
    incident and its communications with stakeholders

V. Financial ecosystem

In addition to our existing actions as described previously in this letter, we have also
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.

*** *** ***

We do not want the technical or operational explanation of what happened to in any way detract
from how seriously we are taking this issue at Visa in the UK, in Europe or at a global level. We
hold ourselves to extremely high standards and are very disappointed that this incident caused
difficulty for consumers and businesses.

We hope you can see from the detail in this letter that we are responding swiftly and thoroughly.
We are not just using this as an exercise to resolve the immediate issue, but as a much wider
learning exercise to ensure that Visa payments work reliably 24 hours a day, 365 days a year. We
are also intending to share our learnings with the broader payments ecosystem, so stakeholders
more generally can better prepare in advance, even for these types of unusual technology failures.

As our financial lives become increasingly digital, it puts into much sharper focus the reliance we
place on the technology and systems underpinning the financial system. We are committed to
ensuring that Visa is continuously setting the best possible standards for prevention, preparation and response. We also recognise the importance of working with all our partners, as we have a collective responsibility to businesses and consumers in the UK and worldwide. That is the standard to which we hold ourselves, and we intend to work across the payments ecosystem, including with our clients, regulators and the government to ensure that as an industry we are all treating technology resilience with paramount importance.

Yours sincerely,

Charlotte Hogg
Chief Executive Officer
Visa Europe

cc John Glen, MP, Economic Secretary to the Treasury; Sir Jon Cunliffe, Deputy Governor for Financial Stability; Hannah Nixon, Managing Director, Payment Systems Regulator
APPENDIX

Visa Europe

Who We Are
Visa Inc. is a global payments technology company that connects consumers, businesses, financial institutions and governments in more than 200 countries and territories, enabling them to use digital payments. Today we connect 3 billion Visa accounts, 46 million retail locations and 16,000 Financial Institutions. The Visa brand stands for acceptance, access, security, convenience, confidence, and universality.

About Visa Europe
Until June 2016, Visa Europe was an independent association owned and operated by European financial institutions. Following the acquisition by Visa Inc., Visa Europe became one of five operating regions (Visa Asia Pacific, Visa CEMEA, Visa LAC, Visa North America). The integration with Visa Inc. brought 3,200 European clients into Visa’s global network of clients and partners.

Visa Europe has separated its scheme and processing activities in accordance with the requirements of the EU Interchange Fee Regulation. In 2015 Visa Europe became a recognised payment system and is supervised by the Bank of England.

Visa Europe currently employs more than 2800 people across the European region, including 2,400 in the UK. Visa Europe also maintain offices in several other European cities including Frankfurt, Paris, Stockholm, Madrid, Istanbul, Warsaw, Milan and Brussels.

We Are Not
Visa is not a bank and does not issue cards, extend credit or set rates and fees for account holders on Visa-branded cards and payment products. In most cases, account holder and merchant relationships belong to, and are managed by our financial Institution clients.

Key Participants in the Payments Ecosystem

<table>
<thead>
<tr>
<th>CARDHOLDERS</th>
<th>ISSUERS</th>
<th>VISA EUROPE</th>
<th>ACQUIRERS</th>
<th>MERCHANTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Individuals and businesses that conduct transactions to pay for goods and services</td>
<td>- Financial institutions or companies that issue Visa products to account holders</td>
<td>- Provides processing and operational systems</td>
<td>- Companies that contract with merchants to accept Visa products</td>
<td>- Retailers, hotels, and others who accept electronic payments as a method of payment for goods or services</td>
</tr>
<tr>
<td></td>
<td>- Assume account holders’ credit risk</td>
<td>- Develop products</td>
<td>- Generate recurring receipts and statements for merchants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Set and collect fees and interest charges from account holders</td>
<td>- Provides risk management</td>
<td>- Provide customer service for merchants</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Provide customer service for account holders</td>
<td>- Builds and manages global brand</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Offer rewards programmes</td>
<td>- Develop new market opportunities (acceptance)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>