POL00397360

HNG X Programme

PCI Incident Response Plan

Author(s)	Richard Barber
Reviewer(s)	POL Head of Information Security (Sue Lowther) HNG Design Authority (Torstein Godeseth) PCI Project Manager (Connie Penn) Security Incident Manager (Alan Simpson) Head of POL Security (John Scott) Live Service and Business Continuity Manager (Gary Blackburn) Head of Product & Branch Accounting (Rod Ismay)
Sign off authority	Sue Lowther
Reference configuration	POL/HNG/PLA/001
Operational Baseline Number	
Version	0.52
Status	Issued
Classification	Working Document
Date	October 2010
Circulation	HNGX Joint Test Team, Operations Control, POL Security teams

POL00397360

1 Document Control

1.1 Version History

VERSION	DATED	CHANGE DETAILS
0.1	18/02/2008	First version of PCI Incident Response Plan
0.2	22/02/2008	Updated following informal review
0.3	29/02/2008	Including comments from informal review
0.4	13/05/2008	Including comments from formal HNGX review Expanded forensic process Added appendix for approved QFIs Added appendix for Streamline incident helpdesk
0.5	27/05/2008	Revised to include Major Incident Alert and further comments from review team Added reference to ACPO Guidelines for computer evidence.

1.2 Change Co-ordinator

All changes to this document are to be sent to the Change Controller below:

Name	HNG Project Support Office
Business Address	148 Old Street London EC1V 9HQ
Business Telephone Number(s)	GRO
Email Address	GRO

1.3 Related Documents

REF.	DOCUMENT REF.	TITLE	VERSION	DATE
1	CON/MGM/006	CMT high level procedures	0.53	
2	S15	RMG Information Security Incident Response Policy (S15)		
3	PCI DSS	Payment Card Industry Data Security Standard	1.1	
4	ACPO Guidelines	Good Practice Guide for Computer-based Electronic Evidence (Association of Chief Police Officers)	4	
5	ISO27001	Information technology. Security techniques. Information security management systems. Requirements	2005	

POL00397360

1.4 Abbreviations

ABBREVIATION	DESCRIPTION
Card Schemes	Means those companies that produce payment cards (credit or debit) e.g. Mastercard, VISA, American Express, Diners Club, JCB etc
CPP	Common Point of Purchase. A term used by the Card Schemes to refer to merchants suspected of being used to compromise payment cards
QFI	Qualified Forensic Investigator. An investigator who has expertise examining computer systems for evidence of malicious activity. For this PCI Incident Response Plan such investigators must be approved by the Card Schemes otherwise they must not be engaged to investigate a PCI Incident. Refer to Appendix A.
FS	Fujitsu Services Ltd
HNGX	Horizon Next Generation
HNGX Data Centre	Fujitsu Services Data Centre(s) used for provision of services for HNGX
IRE11 / IRE19	Fujitsu Data Centres for HNGX. IRE11 is Primary. IRE19 is Secondary
Merchant Acquirer	An organisation, usually a bank, that contracts with one or more Card Schemes to engage and contract with merchants who will accept payment for goods or services by a payment card (credit or debit)
PAN	Primary Account Number. This is the number embossed on the face side of a credit or debit card. Usually 16 digits in 4 groups of 4 but may vary by Card Scheme
PCI	Payment Card Industry
POA	Fujitsu Services Post Office Account (= RMGA)
POL	Post Office Ltd
RMG	Royal Mail Group
RMGA	Fujitsu Services RMG Account (= POA)
SAN	Storage Area Network
User	An employee of Royal Mail Group, a contractor or a third party employee, authorised to access Royal Mail Group information systems for resources or for the purpose of providing IT support or maintenance.

POL00397360

This page intentionally left Blank

POL00397360

Contents

[TOC \o "1-3" \h \z]

POL00397360

2 Introduction

While the POL Major Incident Management process is owned and managed by the Business Continuity Team within Operations Control the PCI aspect is owned by Information Security which manages and escalates a PCI incident as far as possible using processes already established within POL.

A PCI Incident may impact POL in a number of ways. Minor incidents will be handled using established processes within and across POL Security teams.

A Major PCI Incident will require escalation to and management by the Operation Control Major Incident Management Process as defined in document CON/MGM/006.

This document derives from RMG Information Security Incident Response Policy (S15).

2.1 Purpose

The purpose of this document is as follows:

- To define a PCI Incident
- To specify how a PCI Incident should be categorised.
- To define the roles and responsibilities in managing a PCI Incident at its various stages and the methods by which management will be notified and informed of an incident
- To outline the forensic response to a Major PCI Incident
- To define why and when a Major PCI Incident may necessitate the elective invocation of a Major Business Continuity Incident at the HNGX Data Centres
- To identify reporting requirements
- To identify test requirements and propose test scenarios

2.2 Scope

This document applies to POL HNGX programme after it goes live.

This document only applies in respect of the contract between POL and Streamline. It does not apply to any other payment card service used by or for POL.

This document does not apply to suppliers other than Fujitsu Services Ltd Post Office Account.

This document does not apply to any Web Portal.

3 PCI Incident Definition

A PCI Incident is one where information is received that indicates that cardholder data may have been compromised. It is not necessary to demonstrate that cardholder data has been compromised to declare an incident. Part of the PCI Incident Response Plan will be an investigation to confirm whether a compromise has or has not taken place.

POL00397360

PCI Incidents are defined as Minor or Major.

3.1 Minor PCI Incident Definition

The definition of a Minor PCI Incident is not an exact science and will involve the judgement of the POL Security Incident Manager. Such an incident will typically appear to be the work of opportunist theft not organised crime.

Such an incident is one where, for example:

a) Up to 1,000 cardholder details are suspected of being compromised over a period of 12 months or more in four or more locations, AND

b) It can be shown conclusively that a HNGX Data Centre cannot have been involved in the compromise

3.2 Major PCI Incident Alert Definition

The definition of a Major PCI Incident Alert is not an exact science and should involve the judgement of the POL Security Incident Manager and the POL Head of Information Security. The evidence giving rise to an Alert will appear to be an organised activity to obtain credit or debit card details and will necessarily imply large scale compromise of data. Regardless of the volumes of data involved an Major Incident Alert will be raised if any HNGX Data Centre appears to be involved. The suspicion that an HNGX Data Centre is involved will depend on an interpretation of the circumstances surrounding the allegation and the evidence obtained.

Thus a Major PCI Incident Alert is one where, for example:

a) a single large volume compromise appears to have occurred e.g. more than 1,000 cardholder details over a period of no more than one week in four or less locations, OR

b) the evidence indicates that payment card data compromised may have come from POL systems.

c) Where a Merchant Acquirer has announced POL to be a Common Point of Purchase (CPP).

4 PCI Incident Management

This section describes the entry points to the PCI Incident Management Process and the decision points leading to a Minor Incident declaration or a Major Incident declaration.

The process is shown in Figure 1 on page [PAGEREF Figure_1 \h]. and described in Table 1 on page [REF Table_1 \h][REF Table_1 \h][PAGEREF Table_1 \h].

4.1 Initial Reporting

An Initial Report is one made by any POL team receiving an allegation from any source that payment card data may have been compromised while in the possession of POL.

Sources include (but are not limited to): Business Partners, Suppliers or External Agencies, Customers or Users.

POL00397360

It is also possible that the Merchant Acquirer may be the source. This may occur if POL has been identified as a Common Point of Purchase (CPP).

An Initial Report is the first indication received of the possible compromise of cardholder data whilst in the POL environment (counters, business processes, data centre networks, systems, suppliers etc).

Each POL team that may be expected to make an Initial Report must ensure they know what information must be obtained from the source. See Section [REF _Ref191293597 \r \h] and [REF _Ref191302592 \r \h].

4.2 Escalation Path

The Initial Report must be passed to the first person in the list below. That person must respond with a positive written confirmation that the Initial Report has been received and that they are dealing with it.

If no such response is received within 24 hours then the Initial Report must be passed to the next person on the list in exactly the same manner and each time allowing 24 hours for a response.

Escalation	Role
1	POL Security Incident Manager
2	POL Head of Information Security
3	POL Operations Live Service Manager

4.3 Severity Analysis

The person receiving the Initial Report (as defined in the Escalation Path section [REF _Ref191991069 \r \h]) will obtain, confirm and review the evidence of the incident if it is not provided with the Initial Report. It is presumed that such evidence will be a copy of the cardholder data that is alleged to have been compromised. The content and format of the cardholder data may point to how the incident may have taken place.

The POL Security Incident Manager or the POL Head of Information Security must review the evidence and classify the severity of the incident as Minor or raise a Major Incident Alert. See Section [REF _Ref191122514 \r \h].

If the Initial Report has found its way to the POL Operations Live Service Manager their responsibility will be to acquire the evidence as above and ensure that it is reviewed by the POL Security Incident Manager or the POL Head of Information Security. If that is not possible the evidence is reviewed and the incident severity determined as Minor or a Major Incident Alert is issued by the POL Operations Live Service Manager in conjunction with a senior manager within POL who will take responsibility for the incident in the place of the POL Head of Information Security and fulfil all the relevant duties in respect of the incident process.

If no evidence exists then the incident is closed.

The Severity Analysis will be entered into the Incident Report.

POL00397360

4.4 Initial PCI Incident Report

The POL Security Incident Manager is responsible for completing a PCI Incident Report. These reports will use the general incident report format used for all Information Security incidents.

PCI Minor Incident Reports are passed to the POL Head of Information Security and reviewed on a monthly basis.

PCI Major Incident Alerts must be passed to the POL Head of Information Security within one hour of the Major Incident Alert being determined.

4.5 PCI Minor Incident Declaration

Based on the evidence received the POL Security Incident Manager may declare an incident a PCI Minor Incident.

The POL Security Incident Manager will also pass a copy of the PCI Incident Report to the Head of Product and Branch Accounting in the Finance Department so that the Merchant Acquirer can be informed of the incident. The PCI Incident Report remains open until the incident is resolved. The PCI Incident Report must be updated with any progress made and this must also be communicated to the Merchant Acquirer through the normal channels. See Section [REF _Ref191314394 \r \h].

If the Initial Report and the evidence shows that a HNGX Data Centre may be implicated then the incident is automatically a PCI Major Incident.

NB In addition to the PCI Incident Response process all PCI Minor Incidents should be passed to the POL Security (Fraud) Team for investigation of the possible fraud.

4.6 PCI Major Incident Alert

If the person reviewing the evidence decides it justifies a PCI Major Incident Alert the PCI Incident Report must be passed to the POL Head of Information Security within 1 hour of the Alert being issued.

The POL Head of Information Security will review the allegation and the evidence and must confirm or downgrade the Severity Analysis.

If the Severity Analysis is confirmed this is entered into the PCI Incident Report and a PCI Major Incident Alert is issued. This is described in Section [REF _Ref191314464 \r \h].

Once a PCI Major Incident Alert is raised it will necessitate the same process as used by POL Operations for a Major Incident using CON/MGM/006. The circumstances and the evidence will be reviewed by the Working Group which will direct an investigation to confirm whether the Alert merits being escalated to a Major Incident Declaration.

It is required that the Working Group will confer with POL senior management, POL Operations, POL Head of Information Security and the Supplier before electing to declare a Major Incident.

Both the investigation and any subsequent Elective Disconnect must be achieved in a forensically sound manner in accordance with both ACPO Guidelines and the QFI requirements of the Card Schemes. The latter may be found in Appendix D.

POL00397360

4.7 PCI Major Incident Declaration

If the Major Incident Alert is confirmed then the Working Group must issue a PCI Major Incident Declaration. POL then has 72 hours in which to engage a QFI. The decision to initiate and complete the Elective Disconnect of IRE11 will be made by the Working Group as part of the POL Operations Major Incident Management Process.

The Elective Disconnect must be achieved in a forensically sound manner in accordance with both ACPO Guidelines and the QFI requirements of the Card Schemes. The former may be downloaded from the Internet[1][2] and the latter may be found in Appendix D.

The POL Head of Information Security must pass a copy of the PCI Incident Report to the Head of Product and Branch Accounting in the Finance Department so that the Merchant Acquirer can be informed of the Major Incident. The PCI Incident Report must be updated by the POL Head of Information Security as part of the Working Group (see Section [REF _Ref196586554 \r \h]) with any progress made and this must also be communicated to the Merchant Acquirer through the normal channels.

The POL Operations Major Incident Management Process (CON/MGM/006) must be used to manage the incident. See Section 6.

5 PCI Minor Incident Management Process

A PCI Minor Incident will not have occurred within the HNGX Data Centres. However applications hosted within the HNGX Data Centres may have been used to compromise cardholder data.

PCI Minor Incidents could be a result of abuse of Horizon systems, Post Office processes or Supplier systems or processes by POL, RMG or Supplier staff using privileges to obtain cardholder data from Audit, Transaction Enquiry or other systems. Or they could be the result of PO Counter staff falsely obtaining cardholder data at the Counter e.g. through techniques such as "skimming".

The POL Security Incident Manager will obtain, confirm and review the evidence of the incident. It is presumed that such evidence will be a copy of the cardholder data that is purported to have been compromised. The content and format of the cardholder data can point to how and/or where the incident may have taken place.

Minor Incidents will be passed to and investigated by the POL Security Team. The POL Security Team will become responsible for the incident and will report progress back to the POL Security Incident Manager who will update the Incident Report and distribute according to Section [REF _Ref191297306 \r \h].

Whichever team receives a PCI Minor Incident Declaration will investigate the incident following their normal processes and with due regard to safeguarding evidence that may be needed for a prosecution.

6 PCI Major Incident Management Process

6.1 Introduction

In the event of a major incident, activities must be co-ordinated within POL and Supplier businesses in order to minimise adverse impact and protect service to both customers and clients. Due to the large

[1] http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf
[2] http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

POL00397360

number of teams and activities involved this cannot effectively be managed by POL Information Security.

Consequently a PCI Major Incident requires the invocation of the Operations Control Major Incident Management Process.

This process is identified in Operations Control Procedure CON/MGM/006. The highest incident level in that process is Level 3 and is applicable to a PCI Major Incident.

The reason that a Major PCI Incident is automatically a Level 3 Major Incident is because the requirements of the forensic investigation process may necessitate the decision to disconnect the entire data centre from all its connecting networks in order to preserve and analyse the data within for evidence.

The Elective Disconnect is described in [REF _Ref197514729 \r \h] below.

6.2 Differences from Operations Control Procedure CON/MGM/006

This description and the Operations Control Process refers to the 'Working Group'. This is made up of all or specified members of the POL Business Protection Team, as selected by the POL Live Service Team for the specific incident.

The key difference is that a Major PCI Incident **Alert** invokes the POL Major Incident Management Process and convenes a Working Group from the Business Protection Team.

Under this change the Alert is managed as though it were an actual incident to ensure proper management and investigation can take place and to meet the requirements of the Merchant Acquirer and the Card Schemes.

The investigation of a PCI Major Incident Alert and any subsequent Declaration requires the formal engagement of an external company approved by MasterCard and VISA to provide a Qualified Forensic Investigator (QFI). Normally this QFI is imposed by the Card Scheme usually via the Merchant Acquirer. However it is **vital** that POL engage their own pre-selected QFI.

The POL Head of Information Security will maintain a list of POL approved QFI company in Appendix F of this document using the process defined there.

The POL Live Service Team within Operations Control retains the co-ordination point for this incident process.

The POL Head of Information Security must be an active participant in the Working Group. If the POL Head of Information Security is not available they will appoint a substitute and will communicate this to the Live Service Team. If the POL Head of Information Security cannot be contacted then the POL Operations Manager will assume that role supported by members of the Working Group.

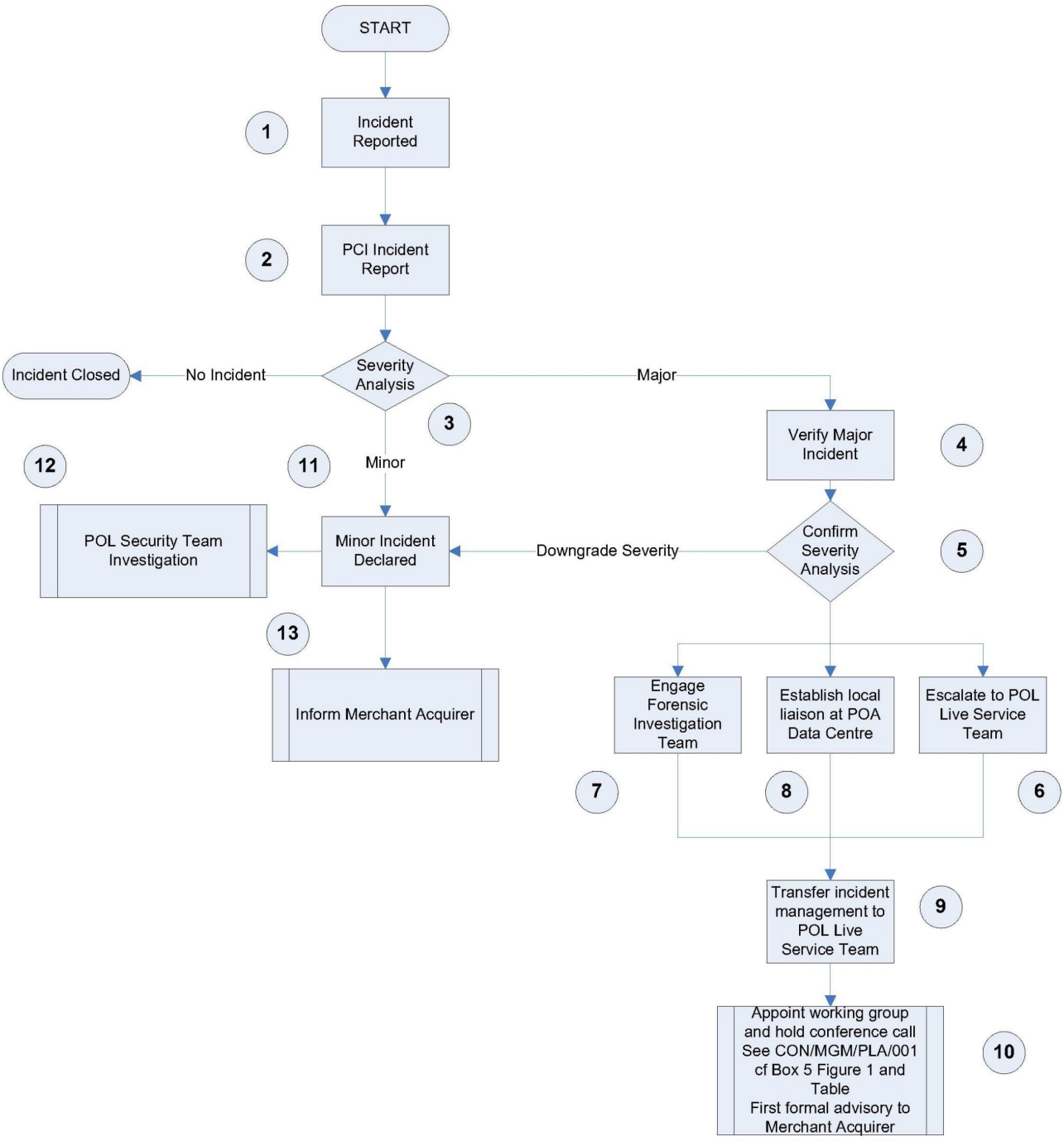
The POL Head of Information Security will report the progress and findings of the forensic investigation to the Working Group established to manage the incident.

The Working Group must ensure that the PCI Incident Report reflects any progress made during the incident investigation and is formally communicated to the Merchant Acquirer via the Head of Product and Branch Accounting.

The POL Security Incident Manager must re-locate to the HNGX Data Centre where the investigation is taking place and act as coordinator and liaison between the POL Head of Information Security, the HNGX Data Centre Incident Response Team and the QFI.

POL00397360

Figure 1: PCI Incident Management Flowchart



POL00397360

Table 1: PCI Incident Management Process

Box	Title	Description	Key timescales	Action owner
1.	Incident reported	Incident identified (clause [REF _Ref191991055 \r \h]) The Initial Report is passed to the POL Security Incident Manager or another member of the Escalation path (clause [REF _Ref191991069 \r \h]). A minimum of 24 hours and a maximum of 72 hours is allowed.		
2.	PCI Incident Report	• The Initial Report is reviewed • Copy of Evidence is obtained • Incident Report opened	Within one business day of Initial Report.	POL Security Incident Manager or alternative
3.	Severity Analysis	Evidence reviewed and incident is: • closed, or • classified as Minor, or • assessed as Major	Within 2 hours of Incident Report being opened	POL Security Incident Manager or alternative
If the incident is Minor impact go to box 11. If the incident is Major proceed to box 4:				
4.	Verify Major incident	Incident Report with Severity Analysis and evidence is passed to Head of Information Security if a Major Incident Alert is issued	Within 1 day of raising a Major Incident Alert	POL Security Incident Manager or alternative
5.	Confirm Severity Analysis	Incident Report with Severity Analysis and evidence is assessed. If downgraded incident passes back to POL Security Incident Manager. If confirmed the Alert is escalated to the POL Live Service Team who will initiate an investigation to determine if a Major Incident Declaration is warranted	Within 1 day of raising a Major Incident Alert.	POL Head of Information Security or alternative
If Severity Analysis is downgraded go to box 11. If the incident is confirmed as Major proceed to box [REF _Ref191302110 \r \h]				
6.	Escalate to POL Live Service Team	• Email Incident Report to POL Live Service Team • follow up with phone call. • Set out PCI Major Incident Management Process requirements should these be needed.	Within 1 day of raising a Major Incident Alert.	POL Head of Information Security or alternative
7.	Engage Forensic Investigation Team	• Select and engage QFI from list of POL approved companies. • Authorise QFI to investigate Alert • QFI will report whether Alert is justified	Within 3 days of raising a Major Incident Alert.	POL Head of Information Security or alternative
8.	Establish local liaison at HNGX Data Centre	POL Security Incident Manager relocated to POA to effect local liaison and incident management with Supplier teams.	Within 3 days of raising a Major Incident Alert.	POL Head of Information Security or

POL00397360

Box	Title	Description	Key timescales	Action owner
				alternative
9.	Transfer incident management to POL Live Service Team	Control of Incident is passed to POL Live Service Team in conjunction with POL Head of Information Security because of specialist security assessments and skills required.	Within 1 day of raising a Major Incident Alert.	POL Head of Information Security or alternative
10.	Appoint working group and hold conference call	The POL Live Service Team appoints a working group to participate in the management of the incident. The working group will be made up of appropriate representatives from the Business Protection Team, relevant POL business/technical managers and appropriate representation from supplier domains [if appropriate]. If Alert is confirmed then a conference call is held and will decide next steps; initiate the Elective Disconnect and compose the first formal (contractually required) communication with the Merchant Acquirer. On direction from the Working Group and MIEG the Head of Product and Branch Accounting will formally communicate the existence of the Major Incident to the Merchant Acquirer through the established channels. Further communication with Merchant Acquirer will be via Head of Product & Branch Accounting at intervals to be agreed with Merchant Acquirer or as directed by Working Group.	Within 1 day of raising a Major Incident Alert.	POL Live Service Team and appointed working group.
Low impact incident [continued from box 3]:				
11.	Minor Incident Declared	• Incident confirmed as Minor on Incident Report. • Copy of PCI Incident Report sent to Head of Product and Branch Accounting for formal communication to Merchant Acquirer.	Within 4 hours of incident being confirmed as Minor	POL Security Incident Manager or alternative
12.	POL Security Team Investigation	POL Security Incident Manager passes control of incident to POL Security Team for investigation (PCI Minor Incidents are managed using existing business as usual processes by the POL Security Team.)	Within 4 hours of incident being confirmed as Minor	POL Security Incident Manager or alternative
13.	Inform Merchant Acquirer	Head of Product and Branch Accounting formally communicates PCI Incident Report to Merchant Acquirer and acts as liaison for future updates to this report.	Within 4 hours of receiving Minor PCI Incident report	Head of Product and Branch Accounting or

POL00397360

Box	Title	Description	Key timescales	Action owner
				alternative
If a PCI Minor Incident escalates to a PCI Major Incident, i.e. the initial impact worsens, then the incident would be reassessed and the process would proceed to box 4.				

POL00397360

7 Reporting

7.1 Initial Reports

An Initial Report is the first indication received of the possible compromise of cardholder data whilst in the POL environment (counters, business processes, data centre networks, systems, suppliers etc).

An Initial Report is a term that describes the details that must be taken when it becomes apparent that cardholder data may have been compromised.

An Initial Report may arise from any Supplier or External Agency or from within POL or RMG.

An Initial Report may be taken by any of the channels that normally receive calls from any party external or internal to POL. Examples of external parties could be Law Enforcement Agencies, Suppliers, Merchant Acquirer, APACS, members of the public, the media – this is not an exhaustive list.

The channels that might receive calls from external parties could be Business Service Centres, RMG Corporate Security Centre, POL Security Team, RMG Portal Webmaster(s), eBusiness team, Horizon Service Desk or National Business Support Centre.

Whichever channel receives a call from an external or internal (POL or RMG) party should log the call using their local procedure and in addition ensure they obtain the details for an Initial Report and then pass the details to the POL Security Incident Manager in POL Information Security.

The details that must be taken for a Initial Report are defined in [REF _Ref191303020 \r \h].

7.2 PCI Incident Reports

PCI Incident reports must be completed and logged by the POL Security Incident Manager using the normal Incident Report format or as otherwise determined. Within any Incident Reports PCI Incidents must be clearly marked as such.

PCI Incident Reports will include all the details of the Initial Report plus the Severity Analysis. Additionally the PCI Incident Report will include a unique Incident number; a summary of the incident, status of incident, issues arising from incident and chase/resolution dates.

The PCI Incident Report must be updated until closed. Updates for Minor incidents must be copied directly to the Head of Product & Branch Accounting for onward communication to the Merchant Acquirer in accordance with the requirements of the contract between POL and the Merchant Acquirer. Updates for Major incidents must be passed to the Working Group and then communicated to the Merchant Acquirer via the Head of Product & Branch Accounting.

PCI Minor Incident Reports are passed to the POL Head of Information Security and reviewed on a monthly basis.

7.3 PCI Major Incident Reports

It is presumed that PCI Major Incidents will only occur within HNGX Data Centres.

The POL Security Incident Manager will complete a PCI Major Incident Report as soon as the incident is declared. This report will be made available to all management involved in deciding how to manage the Incident.

POL00397360

The PCI Major Incident Report must include a unique incident reference (which clearly shows the incident as Major) and will describe the incident, the reason for the severity (which will also describe the evidence), the status and the likelihood that the Data Centres are at risk.

PCI Major Incident Reports will be updated following the process for reporting defined in the Operations Control Major Incident Management Process.

The POL Security Incident Manager will liaise with external organisations involved in the incident e.g. Third Parties, Forensic experts etc in preparing a Post Incident Report. All such liaison will be communicated to the POL Head of Information Security and be communicated via the channels implemented within the Operations Control Major Incident Management Process.

The POL Security Incident Manager will complete and distribute a post-incident report, initially within one week of the incident. Such report will include a root-cause analysis and will be passed to the POL Head of Information Security to approve and distribute to senior management.

8 Testing

PCI DSS requires the plan be tested at least annually. The POL Security Incident Manager is responsible for ensuring that test plans are provided and appropriate.

Test scenarios may be worked into the existing Business Continuity tests and this is preferable for a Major Incident.

Testing must include a scenario where a Merchant Acquirer declares POL is a Common Point of Purchase.

Minor incidents should be tested more frequently and should cover likely scenarios involving low numbers of cardholder details e.g. 100 PANs over 6 months

Tests should at least focus on:

a. ensuring that channels of communication work as expected and are timely

b. ensuring that Initial Reports are accurate and reliable

c. ensuring that evidence is gathered

d. ensuring that severity analyses are conducted; are effective and are appropriate

e. confirming that staff, third parties and especially key suppliers are aware of their responsibilities and have effective incident processes in place

f. confirming that all third party forensic response and capability is appropriate and effective.

g. ensuring that lessons learned are adopted back into the incident process

9 Awareness and Training

PCI DSS requires that appropriate training be given to those with security breach responsibilities. The POL Security Incident Manager is responsible for ensuring that Awareness & Training is planned; that content is appropriate; that relevant staff are trained or made aware and that the POL Head of Information Security received a report on its effectiveness.

POL00397360

The Awareness & Training content needs to ensure, at the least, that the following teams, in POL, RMG and Third Parties, are aware of their roles and responsibilities in the event of a suspected and a declared breach:

a. Security teams

b. Helpdesk teams

c. Operations teams

As a minimum training needs to focus on:

a. Awareness of the importance of and need for Payment Card Industry cardholder data security

b. Appreciation of the potential impact of a Major incident

c. Awareness of the PCI Incident Response Plan

d. How to complete an Initial Report;

e. Ensuring that Initial Reports are passed to correct contact with positive confirmation of receipt

f. Ensuring that incident information is not disclosed to unauthorised parties and especially that POL liability is not admitted

Staff with specialist roles must receive training appropriate to their responsibilities.

POL00397360

Appendix A Payment Card Industry[3]

Card schemes set the business rules that govern the issue of the payment cards that carry their logo. Typically, these rules apply throughout the world to ensure interoperability of cards. In many countries, domestic schemes also operate. The schemes operate the clearing and settlement of payment card transactions. In the UK, banks and building societies must be members of the appropriate scheme to issue cards and acquire card transactions. Examples of international card schemes in the UK are [HYPERLINK "http://www.apacs.org.uk/resources_publications/glossary_8.html" \l "Visa"], [HYPERLINK "http://www.apacs.org.uk/resources_publications/glossary_5.html" \l "MasterCard"], American Express and Diners Club.

A Merchant Acquirer is a bank having a business relationship with merchants, retailers and other service providers to process their plastic card transactions. Acquirers obtain financial settlement from the card issuers, typically via the [HYPERLINK "http://www.apacs.org.uk/resources_publications/glossary.html" \l "card_scheme#card_scheme"] which maintain the clearing systems, and pay the proceeds to the merchant, charging a fee.

The Card Schemes define a security standard on all merchants which is legally binding on all merchants by virtue of their contract with the Acquiring Bank. For the purposes of this document the Merchant Acquirer for POL is Streamline. This standard is the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. At present the design for HNGX falls under these requirements.

The PCI DSS security standard requires a documented incident process for any incident that affects or may affect the security of cardholder data. This documented process is required to be audited and tested annually and must be invoked should it be suspected that cardholder data may have been compromised.

Cardholder data includes all data on the Payment Card or on its magnetic stripe or encoded into the chip if it is a so-called Chip and Pin card. This data includes but is not limited to the: Primary Account Number (PAN), Cardholder name, Service code, Expiration date, Security codes (e.g. CVV2 etc), magnetic stripe data, PIN code etc.

Qualified Forensic Investigators are approved by VISA for investigating breaches of payment card data. VISA maintains this list for themselves. Other Card Schemes also may use this list. The list may be found at [HYPERLINK "http://www.visaeurope.com/"] by searching for the term" Qualified Forensic Investigator".

[3] http://www.apacs.org.uk/resources_publications/glossary_7.html

POL00397360

Appendix B Excerpt from PCI DSS v2 [October 2010]

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.

12.9.1 Create the incident response plan to be implemented in the event of system compromise. Ensure the plan addresses, at a minimum: roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands (for example, informing the Acquirers and credit card associations), specific incident response procedures, business recovery and continuity procedures, data backup processes.

12.9.2 Test the plan at least annually

12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts

12.9.4 Provide appropriate training to staff with security breach response responsibilities

12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems

12.9.6 Develop process to modify and evolve the incident response plan

POL00397360

Appendix C Content of Initial Report

Anyone receiving an initial report must NOT under any circumstances admit any liability for or on behalf of POL and must not pass any personal opinion regarding the incident. At this stage the incident is not confirmed.

An Initial Report must include:

a) Date and time

b) Agent name, contact details and network identifier. An Agent is any person representing Post Office Ltd in receiving an allegation of a compromise of cardholder data in the context of this PCI Incident Response Process.

c) contact details of the person making the report e.g. name, organisation (e.g. Police, member of public, RMG, Supplier etc), landline telephone number, mobile telephone number, address etc

d) Complete description of the cardholder data and format in which it may have been compromised e.g. PANs (Primary Account Numbers – the 16 numbers normal found on the front of the card), cardholder name etc

e) Caller's description of events that indicate a compromise of cardholder data may have taken place.

f) How many card details are thought to be involved

g) How the compromise happened

h) Why the caller believes POL is involved.

i) Agent must ask and record what is the evidence that cardholder data may have been compromised.

j) Agent must also ask for copies of the evidence that cardholder data may have been compromised.

POL00397360

Appendix D Forensic Investigation of PCI Major Incident

Purpose and Background

It is assumed that this Major Incident involves the HNGX Data Centres. It is a contractual requirement on POL that an external and fully qualified forensic team must investigate a PCI Major Incident.

The POL Head of Information Security will maintain a list of approved forensic investigators. See Appendix F. No other forensic team may be involved without the explicit written approval of the POL Head of Information Security or the Working Group otherwise POL risks a breach of contractual obligations which may result in a cessation of payment card processing by the Merchant Acquirer.

The forensic investigators may decide that the incident may only be resolved by an elective disconnect of the Data Centres. The decision to disconnect all or some of the systems that comprise HNGX will necessarily involve the correct level of management via the Working Group.

All parties involved in the PCI Major Incident must support the forensic investigation performed by the Qualified Forensic Investigator. There are mandatory actions performed by the QFI during a forensic investigation which are required by the Card Schemes and which will include the following:

a) Determine the cardholder information at risk

   a. Number of accounts at risk. Identify those stored and compromised on all test, development and production systems

   b. Type of account information at risk:

      i. Full magnetic-stripe data (e.g. track 1 and 2)

      ii. PIN blocks

      iii. CVV2

      iv. Account Number (PAN)

      v. Expiration date

      vi. Cardholder name

      vii. Cardholder address

   c. All data exported by intruder

   d. The timeframe of account numbers stored and compromised

   NOTE: If applicable the QFI must run a packet sniffer on the compromised entity's network

b) Perform incident validation and assessment:

   a. Establish how compromise occurred

   b. Identify the source of the compromise

   c. Determine the timeframe of the compromise

   d. Compromised entity must provide a diagram of the network that includes:

POL00397360

i. Cardholder data sent to data centre

ii. Upstream connection(s) to third party payment processor(s)

iii. Connection to Merchant Acquirer

iv. Remote access connections

v. Specifics on firewall, infrastructure, host and personnel findings

e. Review the entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development and production systems as well as VPN, modem, DSL and cable modem connections and any third party connections

f. Determine if compromise has been contained

c) Check for Track 1 and Track 2 data, CVV2 and/or PIN block storage

a. Examine all potential locations – including payment application – to determine if CVV2 Track 1 and Track 2 data and/or PIN blocks are stored, whether encrypted or unencrypted (e.g. in production or backup databases or tables used in development, application logs, transaction logs, trouble-shooting or exception files, stage or testing environment data on software engineers' machines etc.).

d) If full track data, CVV2 and/or PIN blocks are stored by a payment application, identify the vendor name, product name and version number.

e) Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed.

f) Perform external and internal vulnerability scan

g) Based on their findings the QFI will report to Merchant Acquirer the compliance status for each of the twelve basic requirements under the PCI Data Security Standard.

h) Report findings to the Merchant Acquirer

Process Assumptions

a) There will be a phased approach to forensic investigation of data in HNGX. This would utilise a principle of "least invasive to most invasive".

b) Once a Major Incident is declared POL has 72 hours in which a QFI must be involved in this process.

c) The Working Group convened under the POL Operations Major Incident Management Process will decide whether the Alert justifies declaration of an Major PCI Incident and will take advice on when an elective disconnect of IRE11 and / or IRE 19 might need to happen.

d) The parallel steps i.e. A1, A2 etc, can only take place if there are sufficient QFIs to carry out those steps in parallel. Fewer resources will increase the number of steps needed.

e) Live service from IRE11 and IRE19 will be maintained as long as possible with minimal interruption to service

POL00397360

f) Provision (process and equipment) will be made during an Incident to obtain a forensic copy of data in the SAN in IRE11.

g) The Elective Disconnect will be utilised in order to ensure containment of an incident.

Forensic Investigation Process

A1. Forensic experts (QFI) briefed on design of data centre, network diagram, PCI data flows, storage locations, data formats, audit and logging points, approved memory processes, sockets and protocols etc.

A2. Immediately suspend all planned changes to data centre servers, applications, storage etc. i.e. no code releases, no servers deployed or removed from service.

A3. All admin access to data centre hosts restricted to "four-eyes" access e.g. administrators must be effectively escorted during any access to any host by another administrator.

A4. Initiate an immediate physical security escalation of data centre access. Secure data centre CCTV and access control records, work records etc.

B. Initial Report reviewed by QFIs to determine which systems, transport networks or processes may be out of scope. This is based on a comparison of the evidence against the data in the systems and processes.

C. Based on the Initial Report QFI assess what external links, servers, applications, processes and storage might be compromised. All others placed out of scope.

D. QFI decides what SAN data must be secured and begins activities to identify and secure that data

E. Any external links implicated are physically checked for monitoring tools by external team from POL, assisted by external FS staff and escorted by FS data centre operations manager

F1. QFI review all SYSMAN3 logs

F2. QFI review IRE11 bladeframe server processes in live memory for rogue processes.

F3. QFI copy selected areas of SAN in IRE11 for systems and applications in scope of forensic investigation.

F4. QFI review SAN data for evidence of security breach

G. If none of the above yields sufficient information to exclude the possibility that data has been compromised (and arriving at this stage this is exceedingly unlikely) then elective disconnect of IRE11 is invoked if that is the only remaining option for forensic investigation.

POL00397360

Appendix E Elective Disconnect of HNGX Data Centre

This is a major Business Continuity Event in which a Data Centre is disconnected from its connecting networks in a planned and organised manner.

It is similar to a major Business Continuity Incident but is different in that it is planned and is forced by the requirement to comply with an obligation under contract with the Merchant Acquirer.

The purpose of the Elective Disconnect is to ensure that no network based process or traffic may deliberately or unintentionally change the state of the processes or data in the affected environment.

The consequences of not complying may be the withdrawal of the facility to process card transactions under that contract. This in itself may not have the same overall effect on POL operations at the Counters as disconnecting the Data Centre(s) but which may endure for a good deal longer. Whether this would be the case and how much longer it would last depends almost entirely on negotiation with the Merchant Acquirer.

The worst case scenario is one where the Merchant Acquirer is not influenced by outside pressures or negotiation and denies POL the facility to process any relevant payment card transactions until satisfied that the security breach has been completely identified; that the breach did not compromise or no longer compromises cardholder data.

Relevant payment cards are those falling under the contract with that Merchant Acquirer. In the scope of this PCI Incident Plan that would be Streamline.

Planning the Elective Disconnect

This ideally would have already been completed by the Data Centre supplier. It should form part of the annual test of this plan.

The disconnect must identify two scenarios:

a). The Primary Data Centre must be disconnected from all external networks e.g. Fujitsu corporate network, the internet, the POL Counters environment and any other Data Centres.

b) Specific systems within the Data Centre must be disconnected from internal networks as advised by the QFI.

Any disconnection must be achieved in a forensically sound fashion and with due regard for the need to contain an incident.

It should also include a planned re-connection. It might be assumed that would be the same as bringing the Data Centre(s) back online after a major BC incident. However a test would demonstrate whether this would be the case or not and a test should therefore be undertaken.

POL00397360

Appendix F POL Approved QFIs

This is the formal list of those Qualified Forensic Investigators which have been assessed by POL and considered experienced to handle the forensic investigation of the HNGX data centres.

F.1 Requirements for POL Approved QFI

The key considerations for the formal approval by POL of a company capable of the forensic investigation of HNGX data centres are threefold:

1. First and foremost the company offering forensic investigation services must hold a current approval from VISA as a PCI Qualified Forensic Investigator. This may be confirmed independently by referring to the VISA website at [HYPERLINK "http://www.visaeurope.com"][4] and then obtaining the most up to date QFI list by searching[5] for the term "Qualified Forensic Investigator". The current Master Card QFI list must be obtained from Master Card as it is not a public document.

2. The company offering QFI services must appear on the POL Preferred Suppliers List

3. The QFI must have a separate commercial contract for the provision of services as a QFI quite apart from any other commercial contract for any other services which the company may provide.

4. The QFI must satisfy the POL Head of Information Security that they are capable and experienced in the forensic investigation of virtualised bladeframe and SAN environments

5. The QFI must satisfy the POL Head of Information Security that they are familiar with and fully support the process described in [REF _Ref191123384 \r \h * MERGEFORMAT] "Forensic Investigation of PCI Major Incident".

F.2 Responsibilities of POL Head of Information Security

It is the responsibility of the POL Head of Information Security to:

a) Correctly assess a candidate QFI for inclusion on the list according to the criteria set out above in [REF _Ref196630398 \r \h]

b) Ensure that the list is kept current and that the details are accurate and complete.

c) Ensure that all key parties are informed of the latest list when it has been updated

d) In the event of a PCI Major Incident to select a QFI from the list; confirm this selection with senior management (if need be) and communicate this selection to the Working Group and other key parties e.g. Merchant Acquirer, Fujitsu RMGA, IRE 11 and 19 Data Centre Operations Manager etc.

This is important because in the event of a PCI Major Incident affecting HNGX data centre other parties in POL or Fujitsu may refer to this list and select a QFI from it in the absence of the POL Head of Information Security.

---

[4] It is very important that this search only be performed on the [HYPERLINK "http://www.visaeurope.com"] website since VISA Europe is a separate legal entity from any other VISA organisation.

[5] It is also very important that this search be performed from the [HYPERLINK "http://www.visaeurope.com"] website as other search engines may return an out-of-date QFI list.

POL00397360

Selecting a QFI that does not meet the necessary criteria given above may cause unnecessary delays to the incident management process or at worst compromise the effectiveness of the investigation and potentially bring harm to POL and/or RMG brand.

F.3 List of POL Approved QFIs

List of POL Approved QFIs	
Company	Contact
	Name: Email: Phone:
	Name: Email: Phone:
	Name: Email: Phone:

POL00397360

Appendix G How to Contact Streamline

The text in this section has been reproduced from the Streamline Merchant Operating Instructions which may be found online[6].

What to do if data is compromised

If you believe that cardholder information has been obtained by an unauthorised person or company, this fact must be reported to Streamline as soon as possible together with details of all the account numbers involved and all the circumstances of the compromise.

Acting promptly to notify us and limit the possible consequences after a compromise incident has occurred is vital.

Have a business continuity plan in place should a data compromise be identified, whether the problem is in your own systems, or as a result of a support failure, or a failure by another organisation with which you share information.

Should you encounter or suspect a cardholder information compromise, please notify the Streamline Merchant Helpdesk on GRO*.

* Max call charge from BT landline is 3p per minute. Calls from other networks may vary. Telephone calls may be monitored and recorded to improve our service.

The opening hours are:

1. 8 a.m. to 8 p.m. Monday to Friday
2. 9 a.m. to 6 p.m. Saturday
3. 10 a.m. to 4 p.m. on Sundays
4. 9 a.m. to 5 p.m. on Bank Holidays

An answer phone message is in place outside of these hours. Calls may be recorded.

[6] http://www.streamline.worldpay.com/support/kb/moi/moi.html#moi5100.html

POL00397360

Appendix H Information Flows

This diagram illustrates where an allegation may enter POL and once inside POL where it may be routed until it reaches the POL Security Incident Manager (Information Security).

The routes from Compliance and Product & Branch Accounting are different in that one tracks movements of large transactions and so is internally generated and the other relates to a Common Point of Purchase (CPP) declaration coming from a Merchant Acquirer via their contact in P&BA.

All these flows describe what are current information or escalation processes within POL.

POL00397360

Figure 2: PCI Information Flowchart