

To: Jonathan Gribben[GRO]; Lucy Bremner[GRO]; Andrew Parsons[GRO]; Emma Campbell-Danesh[GRO]
Cc: Gareth Jenkins[GRO]; Ibbett, Dave[GRO]; Newsome, Pete[GRO]; Parker, Steve[GRO]; Jay, Christopher[GRO]; Godeseth, Torstein[GRO]
From: Lenton, Matthew[O=FUJITSU EXCHANGE ORGANIZATION/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=87F95ED0A28548A8BD569F2CB6F]
Sent: Mon 2/11/2019 10:08:26 AM (UTC)
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Jonny,

Please see below the responses from Gareth, in his email of the 9th Feb, and also the notes that are appended to Jonny's email of the 6th, at the foot of this chain. Note also the document references, which Gareth refers to, in the email from me on the 8th Feb.

Matthew Lenton
 Post Office Account Document Manager
 P&PS, Digital Technology Services

Fujitsu
 Lovelace Road, Bracknell, Berkshire, RG12 8SN
 Phone: [GRO]
 Email: [GRO]
 Web: <https://www.fujitsu.com/global/>

From: Gareth Jenkins [GRO]
Sent: 09 February 2019 11:27
To: Lenton, Matthew <[GRO]>; Ibbett, Dave <[GRO]>; Newsome, Pete <[GRO]>; Parker, Steve <[GRO]>; Jay, Christopher <[GRO]>; Godeseth, Torstein <[GRO]>
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

IMPORTANT - This email or attached documents contains legal advice (or relates to litigation or anticipated litigation) and is being provided in circumstances for which Legal Privilege may be claimed. Do not copy or forward this document without permission.

Hi,

Thanks for these docs Matthew.

I've had a quick scan and they confirm the following:

1. All AP Transactions in Old Horizon were digitally signed at the counter and so cannot be spoofed by SSC
2. All Banking Transactions are digitally signed at the counter and so cannot be spoofed by SSC
3. (NB all transactions are digitally signed in HNG-X so spoofing can't happen).

That means that the only transactions that could possibly be injected by SSC to benefit them (as opposed to re-injecting copies of missing transactions that have been recovered) are EPOSS Transactions, which mean Giro Deposits and Manual Banking Deposits.

You might want to pass the good news onto Jonny.

Best wishes

Gareth

From: Matthew.Lenton[GRO]
Sent: 08 February 2019 10:42
To: Dave.Ibbett[GRO]; Gareth Jenkins <[GRO]>; pete.newsome[GRO]; ParkerSP[GRO]; Christopher.Jay[GRO]; Torstein.O.Godeseth[GRO]
Subject: RE: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Gareth,

Attached is
AD/DES/020 Automated Payment System Agents for Release B13 High Level Design
AD/DES/065 High Level Design Specification for Network Banking Agents
AD/DES/067 Network Banking Authorisation Agent Design

From: Jonathan Gribben [GRO]
Sent: 06 February 2019 21:05
To: Gareth Jenkins <[GRO]>; pete.newsome [GRO]; Christopher.Jay [GRO]
Legal.Defence [GRO]; ParkerSP [GRO]
Subject: FW: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Splitting attachments.

Jonathan Gribben
Managing Associate
Womble Bond Dickinson (UK) LLP

d: [GRO]
m: [GRO]
t: [GRO]
e: [GRO]

[Stay informed: sign up to our e-alerts](#)



womblebond dickinson.com



From: Jonathan Gribben
Sent: 06 February 2019 20:01
To: 'Gareth Jenkins'; 'pete.newsome' [GRO]; 'Christopher.Jay' [GRO]; 'Legal.Defence' [GRO]
Cc: Andrew Parsons; 'Dave.Ibbett' [GRO]; Lucy Bremner; 'ParkerSP' [GRO]; Emma Campbell-Danesh
([GRO])
Subject: Injecting transactions - urgent [WBDUK-AC.FID27032497]

Dear all,

Privileged & Confidential – please do not forward

Apologies in advance for the length of this email.

Exec Summary

Paragraph 35 of Steve's second statement is not entirely correct. We have been looking into this subject further and below is a summary of our investigation.

We need to send Freeths a letter to clarify the correct position. I have summarised the key points and set out some questions below along with a summary of our investigation. Please would you review those let me know the responses/whether anything is incorrect by midday tomorrow. Once this has been done we will draft a letter to Freeths correcting the position that we will ask you to review and confirm before it is issued.

Summary of key points/questions

Key points:-

- Post Office offered personal banking (manual) for a number of institutions from the introduction of Horizon;
- it would have been possible for a rogue SSC employee to inject a cash deposit into their personal banking account;
- a customer's account would not be credited until the paper deposit slip reached the relevant financial institution (need to confirm this for Girobank), so the rogue SSC employee would not benefit from injecting a transaction because there would be no corresponding paper deposit slip (query whether a TC would be issued due to the absence of the paper deposit slip);
- online banking transactions were introduced in 2003 and Gareth does not know if it would even be possible to get around the encryption issues that would be present if someone tried to insert an "automated" transaction; and
- there are some other transactions that the rogue SSC employee could have injected – for manual transactions there may be a paper trail (TBC on a transaction by transaction basis) and for online (i.e. automated) transactions the position would be the same as per online banking transactions (i.e. encryption issues).

Questions:-

- were online Girobank transactions AP transactions? [GIJ] no. They were EPOSS Transactions. However the distinction isn't particularly important. With AP transactions, a copy of the transactions is sent to the client. With EPOSS they aren't, so POL do the reconciliation based on data received from the Banks.
- does AP mean automated?; [GIJ] yes AP stands for Automated Payments. However, that is nothing to do with the distinction between Automated and Manual Banking Transactions. Not sure where the term AP comes from – need to ask POL.
- what would a rogue SSC employee have to do to in order to inject an online/automated transaction (i.e. please articulate the encryption issues and describe what would have to be done to theoretically get around them, including references to any controls designed to prevent this)? [GIJ] I can't remember exactly how the detailed crypto checks worked on NBS. Would need to check the documentation. I believe that there was something generated by the Pin Pad and also the message was digitally signed using a key known only to the counter, but it needs checking out. I doubt if SSC would be able to spoof such a message, but can't say 100% (just 99.9%)

Summary of investigation into injecting transactions in Legacy Horizon

Paragraph 35 of Steve's statement reads:-

"With reference to Dr. Worden's statement that "as for transferring money, Horizon includes no functionality that allows payments to be made to external parties or account", at paragraphs 20.1, 20.3, 21 and 58.4 of my first statement I said that money could not be transferred, by which I mean that it could not be transferred into a third party's bank account. I have given this matter further thought and discussed it with my colleagues and we have now theorised that someone could have carried out a Post Office transaction, such as a GIRO bank transfer² or a utility bill payment. A GIRO bank transfer inserted by someone at SSC would have been detected as part of Post Office's reconciliation processes because there would be no accompanying paper document. There is no accompanying paper document for a utility bill payment, so in theory such a transaction would not be detected through reconciliation. I am not aware of any such activity ever taking place and if it had occurred it would have resulted in instant dismissal.

2 A Giro bank is also an AP transaction (like bill payments). It is the only type of bank account that is. All other banking deposits go through a totally different path."

After the statement had been submitted, Gareth provided the following comments:- [GIJ] I agree with these statements and did send them to Jonny.

1. The Giro Bank Transactions are not AP, but standard EPOSS Transactions. I don't know how info on them got to Giro Bank – it may well be that Giro Bank worked off the paper trail and then sent summaries to POL which they then reconciled with the Horizon feed. POL would need to provide the details.
2. Prior to online banking (introduced in 2003), POL did support some (but not all) other banks with deposit and cheque cashing facilities. Again these were EPOSS (not AP) transactions. I assume that there was also a paper trail here and it would work in a similar way to Giro Bank. Again it is POL that need to define the process. All Horizon did was provide the buttons to record the electronic part of the transaction.

Please find attached the following documents:

1. Post Office's Counter Operations Manual for Personal Banking (version 1 August 2001) which sets out the procedure for accepting cash deposits other than Alliance & Leicester Giro services (see the comment on page 2 re Alliance & Leicester Giro services being distinct and separate from those that appear in this booklet and can be found in the Alliance & Leicester Giro booklet – Post Office have not yet been able to locate the corresponding version of this booklet but has provided version 3 from March 2007 – see point 3 below) and states that cash is not deposited into a customer's account until the paper deposit document reaches their bank (section 5.9 on page 9).

2. Post Office's Operational Focus 0203 from 3 – 9 April 2003 which contains a list of banking services available at branches from Tuesday 1 April 2003 and shows that Post Office accepted cash deposits from seven banks. All of them are stated to be "manual", apart from Alliance & Leicester/Giro Bank which is stated to be "automated or manual". Manual means paper based and automated means online using a card.
3. Post Office's Operations Manual for Alliance & Leicester Personal Banking (version 3 March 2007). This version shows that Post Office did not offer manual Alliance & Leicester personal banking by March 2007 – it was online banking only.
4. Post Office's Horizon System User Guide / Balancing with Horizon Guide (version 1 28 July 2000). This Balancing with Horizon Guide Section 1 deals with Personal Banking (page 734 of the PDF) and Alliance & Leicester Girobank (page 743 of the PDF). It was a requirement to rem out paper deposit slips on a daily basis. There was also an opportunity for branches to reconcile the Horizon record of deposit transactions with the paper deposit slips they were holding as part of this process.

The distinction between online and manual banking transactions is that it would have been possible for SSC to insert a "manual" transaction, but Gareth does not know if it would even be possible to get around the encryption issues that would be present if someone tried to insert an "automated" transaction. Automated deposit transactions required the customer's card to be swiped through the PIN Pad, which would add in some crypto data that prevents SSC being able to mimic this step. [GIJ] yes, I agree with this, but perhaps we need to be more specific to prove why it couldn't be mimicked. **[Matthew Lenton]** I think this is added to by Gareth's response at the top.

In terms of other transactions that could have potentially been injected for personal benefit, based on the list of products and services available in branches as at July 2005 as per the attached welcome pack Gareth has advised that:-

- it may have been possible to inject bill payment transactions to pay a bill (i.e. the utility bill example given in Parker 2, for which there would be no paper trail/reconciliation); [GIJ] yes we have agreed that
- telephony transactions were all online, so the position is the same as online banking transactions (i.e. encryption issues); [GIJ] agreed
- banking/savings – covered above; [GIJ] agreed
- national savings and investments – a mix of online and offline. We are checking with Post Office whether there was a paper trail for the offline ones; [GIJ] agreed
- money transfer – online; and [GIJ] agreed
- the rest did not involve any accounts to credit and therefore the rogue SSC employee wouldn't benefit. [GIJ] agreed

Please consider the environment! Do you need to print this email?

The information in this e-mail and any attachments is confidential and may be legally privileged and protected by law. [gi.jenkins@wbd.co.uk](#) only is authorised to access this e-mail and any attachments. If you are not [gi.jenkins@wbd.co.uk](#), please notify [jonathan.gribben@wbd.co.uk](#) as soon as possible and delete any copies. Unauthorised use, dissemination, distribution, publication or copying of this communication or attachments is prohibited and may be unlawful. Information about how we use personal data is in our [Privacy Policy](#) on our website.

Any files attached to this e-mail will have been checked by us with virus detection software before transmission. Womble Bond Dickinson (UK) LLP accepts no liability for any loss or damage which may be caused by software viruses and you should carry out your own virus checks before opening any attachment.

Content of this email which does not relate to the official business of Womble Bond Dickinson (UK) LLP, is neither given nor endorsed by it.

This email is sent by Womble Bond Dickinson (UK) LLP which is a limited liability partnership registered in England and Wales under number OC317661. Our registered office is 4 More London Riverside, London, SE1 2AU, where a list of members' names is open to inspection. We use the term partner to refer to a member of the LLP, or an employee or consultant who is of equivalent standing. Our VAT registration number is GB123393627.

Womble Bond Dickinson (UK) LLP is a member of Womble Bond Dickinson (International) Limited, which consists of independent and autonomous law firms providing services in the US, the UK, and elsewhere around the world. Each Womble Bond Dickinson entity is a separate legal entity and is not responsible for the acts or omissions of, nor can bind or obligate, another Womble Bond Dickinson entity. Womble Bond Dickinson (International) Limited does not practice law. Please see www.womblebond Dickinson.com/legal notices for further details.

Womble Bond Dickinson (UK) LLP is authorised and regulated by the Solicitors Regulation Authority.

Unless otherwise stated, this email has been sent from Fujitsu Services Limited (registered in England No 96056); Fujitsu EMEA PLC (registered in England No 2216100) both with registered offices at: 22 Baker Street, London W1U 3BW; PFU (EMEA) Limited, (registered in England No 1578652) and Fujitsu Laboratories of Europe Limited (registered in England No. 4153469) both with registered offices at: Hayes Park Central, Hayes End Road, Hayes, Middlesex, UB4 8FE. This email is only for the use of its intended recipient. Its contents are subject to a duty of confidence and may be privileged. Fujitsu does not guarantee that this email has not been intercepted and amended or that it is virus-free.