FUJ00155534

From: Orzel Brian F[/O=ICL/OU=UKSOUTH FEL01/CN=RECIPIENTS/CN=ORZELB]

Sent: Thur 22/11/2001 3:44:30 PM (UTC)

To: Pope John[GRO]; Hollingsworth David[GRO]

Cc: Morrison Ian[GRO]; Jenkins Gareth GI[GRO]; Jarosz Mark[GRO]; Hooper Graham J[GRO]; Wright Walter[GRO]

Subject: Draft Response V3 RE: Transaction reference

Attachment: jury.txt

Incorporates suggestions from Gareth. As I feared, audit trail is not quite "for ever". He suggests that getting Mike Murphy to underwrite it is overkill. Graham can not look at it until tomorrow or later, Mark will look at it soon, and Walter is happy. Graham points out that case by case legal support is a chargeable revenue stream. Hmmm.... Wonder what margin we can make on my time....

Brian

I have attempted to give a comprehensive and fully accurate answer.
The request said "not too technical" I have done my best, but only with moderate success.
You may consider me too frank, wordy or politically inept, if so I invite feedback

Brian

to: john.plowman GRO
cc: Pope John

John,

I think the following would be the most accurate, understandable and complete approach. I apologise for its length. You could summarize or dumb it down further for a jury, but maybe at some risk under cross examination. (I am a technical expert rather than a barrister and can not really advise upon this aspect!)

The Post Office computer system is based upon a journal, (also known as a message store or audit trail) a copy of which is kept on every counter within a post office and on a sufficient number of central site machines and archives.

This journal is "Append only". What this means is that the computer can record a new message in the journal, but cannot modify an existing one.
(Any failed attempts to do so are recorded in an audit trail, and are of sufficient importance that they too are recorded centrally.)

The entire journal is identified as being generated within the United Kingdom (44) rather than any other country using the same system.

Every Post Office is given a unique identifier within the United Kingdom (The "GroupId")

Every counter within the Post Office is given a unique identifier within the post office. (The "Id")

Every message generated on the counter is given a unique number which increments by precisely one for each new message. (The "Num")

Every message also contains a check against corruption.

FUJ00155534

(Confidential cryptographic measures are taken to ensure the reliability of the above identification.)

Therefore if you look at such a log, there is a clear and easily understood sequential audit trail of exactly what messages were recorded on the counter.

(I enclose an example)

Note the unique start of each message within the audit trail:

<Message:<GroupId:901777><Id:1><Num:7994>
<Message:<GroupId:901777><Id:1><Num:7995>
<Message:<GroupId:901777><Id:1><Num:7996>

The integrity of this sequencing is at the absolute core of the product that the post office uses, and can be trusted more than anything else.

The product is also able to produce a "Unique Identifier" upon demand. This consists of a string of characters, for example "44-901777-1-7992-3". The tail end of such an identifier might be used as a "Transaction Reference", but it might also be discarded (A) or used for a variety of other purposes(B), some of which would not be obvious to a counter clerk. The manufacturer does not specify how they create this unique identifier, nor its length or internal structure, or any kind of sequential pattern. (C) the pattern is also very noticeably broken when the task of work is moved to and from another machine. (D) Furthermore routine maintenance may be going on on the machine simultaneously, and it too may "consume" some of these unique Identifiers.(E)

There is a common assumption that the internal structure of the example given consists of the "44-" for the country, "901777-" for the post office (GroupId), "1-" for the counter (Id) upon which the current batch of work started (it could have moved to another counter since) "7992-" for a fairly recent message "Num" and "3" for a trailing unique number that just gets bigger. This assumption is erroneous. The manufacturer has never specified how the unique identifier is generated, and the technique they use has changed from time to time. (F)

Taking A, B, C, D, E and F into account, it is therefore perfectly normal that if someone were to make such an invalid assumption they might think that transactions were "missing". To do so would be to jump to an invalid conclusion. Tracing back from the report to the underlying journal however will always reveal the truth.

The journal uses the full "44-901777-1-7992-3" style unique identifier, whereas the Transaction log abbreviates it thus: "1-7992-3"

The "Transaction log" is more easily understood by a human being, but is a derivative report generated from the journal. This means that it is subject to fraud, misrepresentation error or archiving. The clearest and simplest way to perform such a fraud would be to "borrow" the printer and attach it to a domestic PC. Reports produced centrally from the audit subsystem are more reliable in this respect.

However there is a clear and self evident relationship between the Transaction log and the underlying journal, so such fraud is trivial to detect.

At the central site, the audit trail is maintained for a very substantial period of time. For practical reasons, older material in the local copy at the counter is purged after a period of time. Such purging stands out very clearly in the audit trail as missing messages, but it does mean that there is a slight risk that if a transaction log report is generated substantially after the event it may omit archived messages and thus give misleading results.

Contrariwise, because we keep a long term audit trail centrally, the counter staff may misguidedly assume that once a transaction has "dropped off" the "transaction log" they are "safe" - They could be in for a nasty surprise, the audit subsystem can re-create such reports for any time period with ease.

FUJ00155534

For all these reasons I would strongly recommend that any court case relying upon "transaction log" reports also provided the raw and unadulterated underlying message store extract as evidence.

Indeed, for the avoidance of all doubt I would ask you to consider avoiding the transaction log altogether and to consider presenting the raw audit trail complete with an attached commentary targeted at the jury. The central auditing subsystem is specifically targeted at producing such reports. I suspect this would give an inventive defence barrister much less scope. My experience is that the layman can readily understand the essential underlying simplicity of the raw audit trail with ease, but might be a confused by the detail without guidance.

With Pathway's approval I would be more than delighted of offer specific case by case expert advice if required or to chat through the issues directly with the person involved.

Brian Orzel

-----Original Message-----
From: john.plowman GRO
[GRO]
Sent: 22 November 2001 09:55
To: John.Pope GRO
Subject: Transaction reference

John

I have received a query regarding the logic supporting transaction referencing as it appears on a Transaction log report. The person requesting this information has to attend court from time to time to respond to claims made by suspended counter staff that apparent 'gaps' in the numbering sequence indicates that supporting evidence cannot be relied upon. Whilst I was able to offer some advice on the subject I was wondering if there is a document around that could be of help here?
Alternatively is there somebody who I could talk to on the subject?

Regards

John Plowman