Workpaper reference: D.2

Source: AuditBoard.

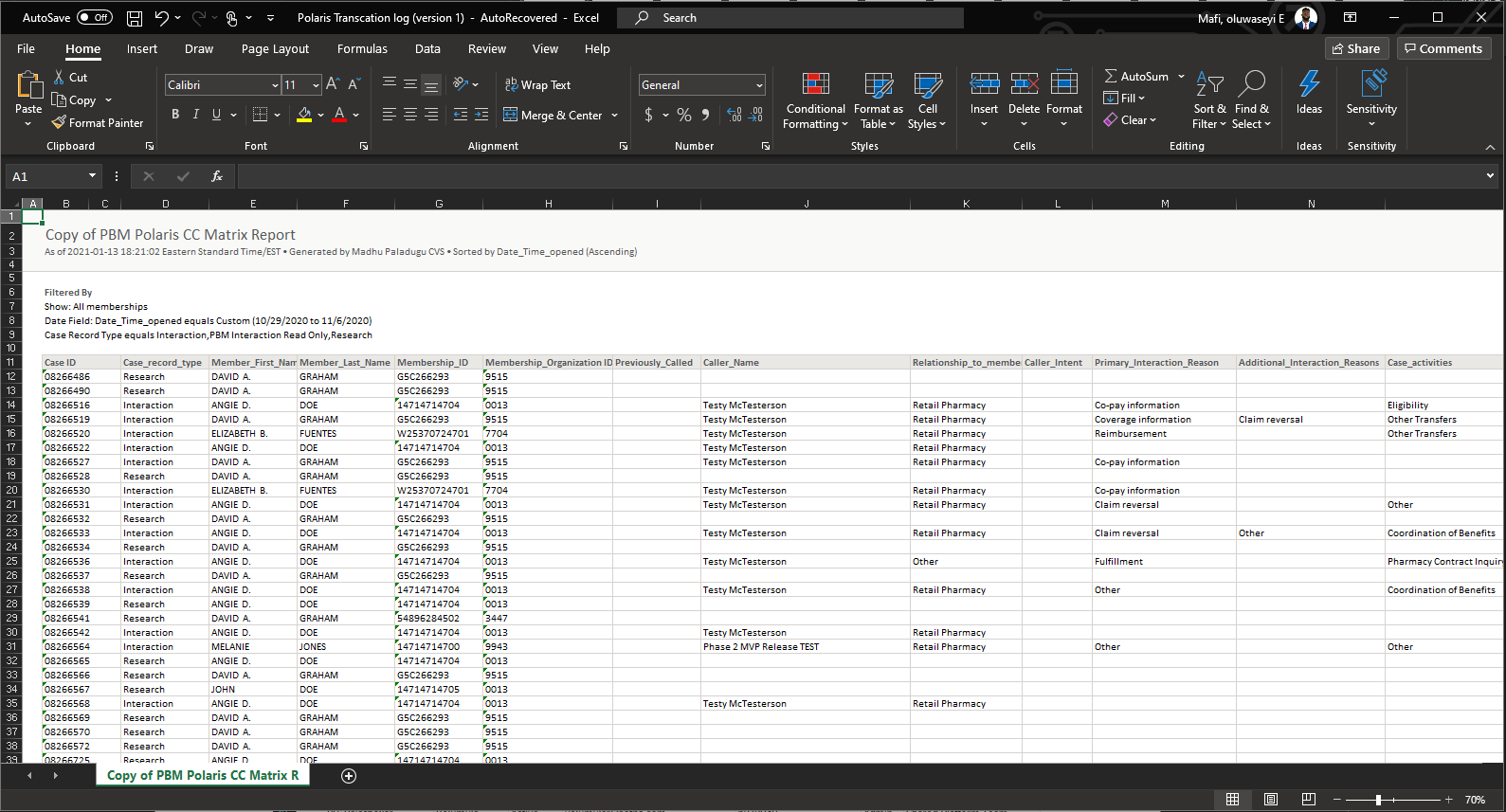
Provided by: Madhu Paladugu, Sr. Advisor, Application Development

Date: 1/13/2021

Description: The attached screenshot below shows a system generated transaction data log for Polaris (List 1) from the week of October 29, 2020 to November 6, 2020. This is also the time frame when Polaris pilot started. Also included below is a screenshot of the query of how this transaction data log report was produced (List 2). Additionally, screenshot (List 3) captures potential PHI and PII drawn from the transaction log data. (List 4) shows the web application manager’s interface showing data is secured and encrypted at rest.

IA Notes: The attached screenshots below show that there are potentially sensitive data such as personal information, health related documentation, medical prescription dosage which can be tied to the caller as the individual inquiring for requested information (See D2.2); however, additional evidence shown in (List 4) prove that these potentially sensitive data within Polaris is secured and encrypted at rest on the database.

Attribute A

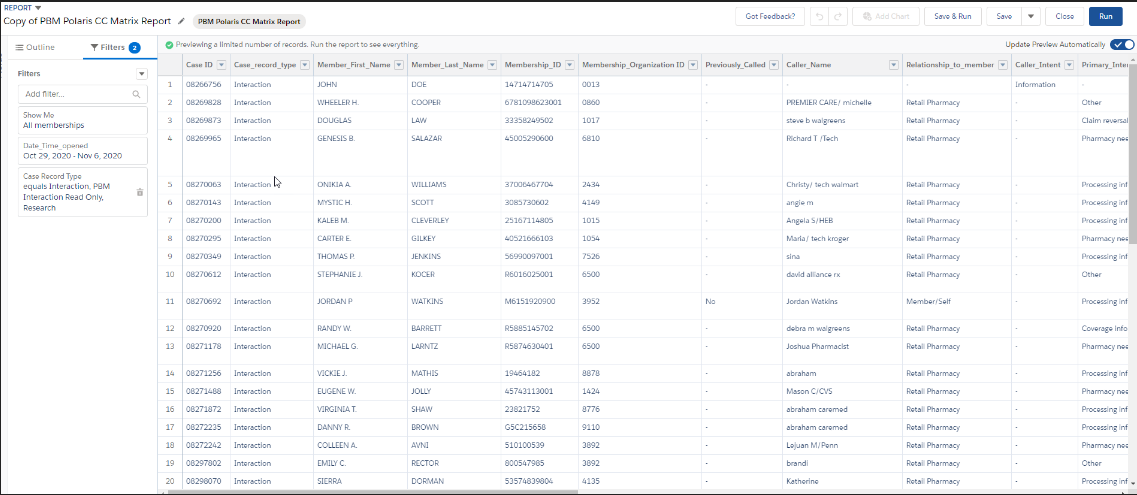


List 1: Listing of all the records inputted in Polaris within the time frame in scope (Oct 29,2020 to Nov 6, 2020)

D2.1

IA observed that the personnel that ran these query search had appropriate permission to obtain information, the right database selection is in scope and the search filter used showcase a request for all member within Polaris

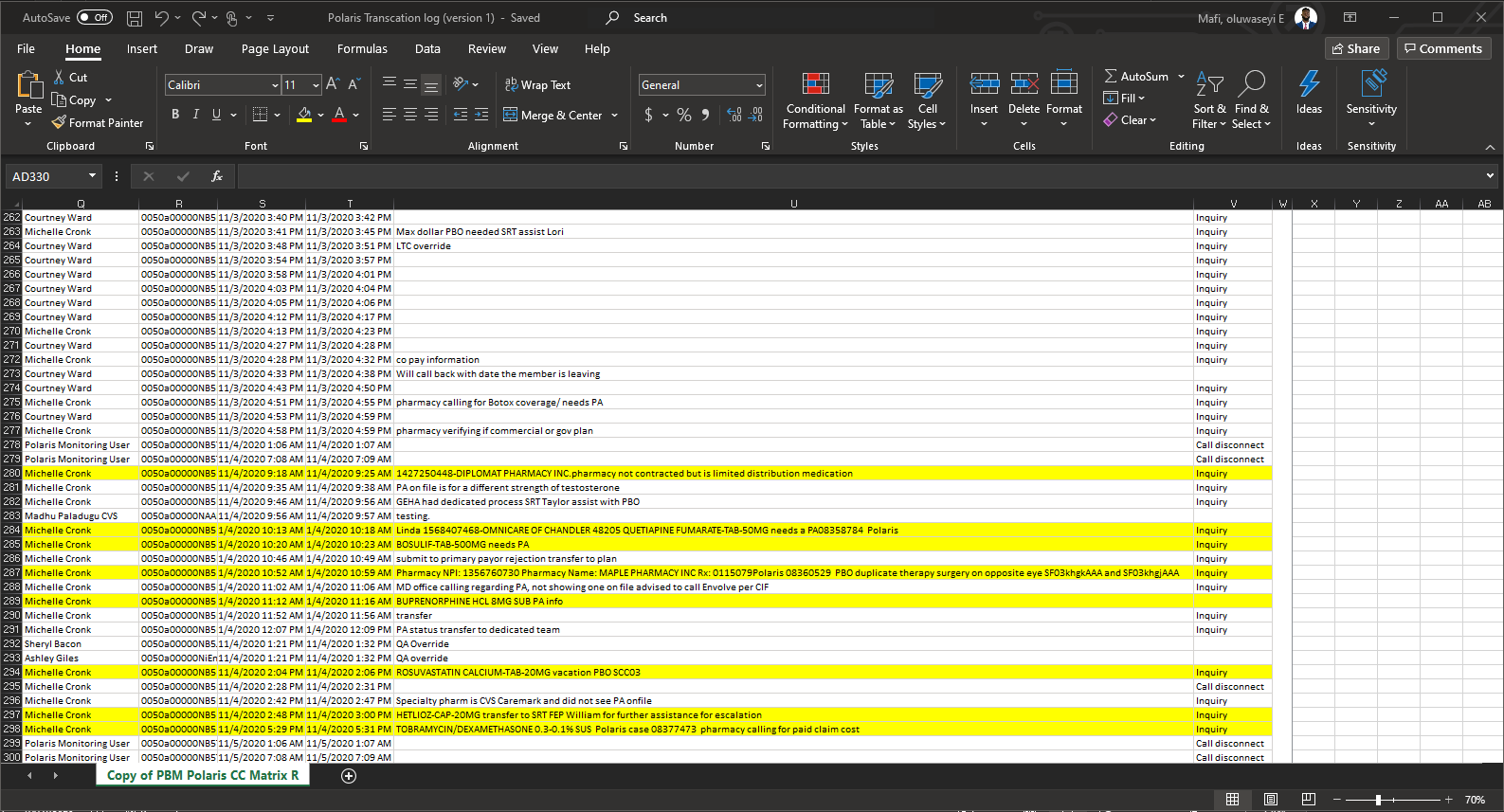
that the individuals in both lists were not the same, during a VLOOKUP exercise.

List 2: Screenshot showing the query filters used in generating the record above (List 1)

D2.2

IA reviewed 100% sample of data in column U within the transaction log. This section includes information ‘case comments.’ IA observed that certain information pulled out of the transaction log included potentially sensitive data such as personal information, health related documentation, medical prescription dosage.

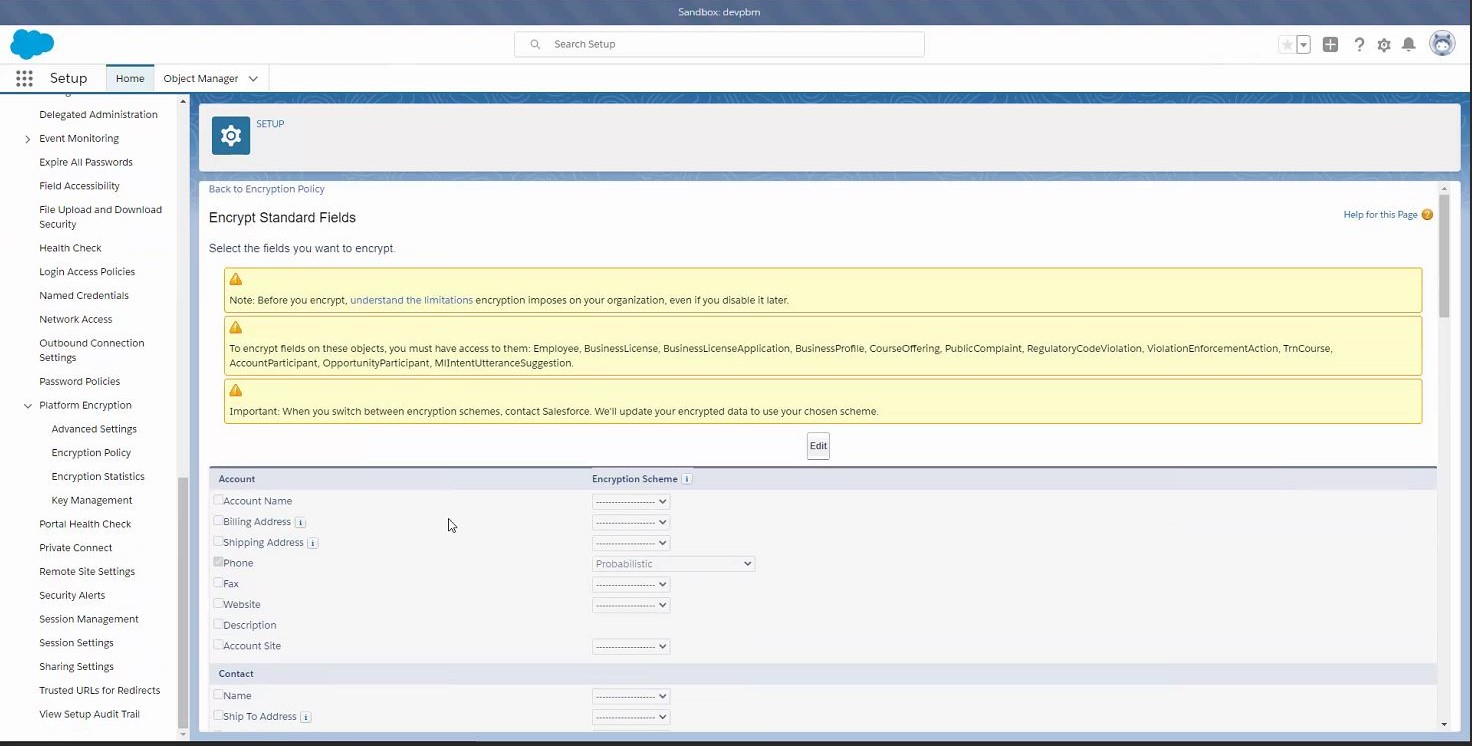
that the individuals in both lists were not the same, during a VLOOKUP exercise.

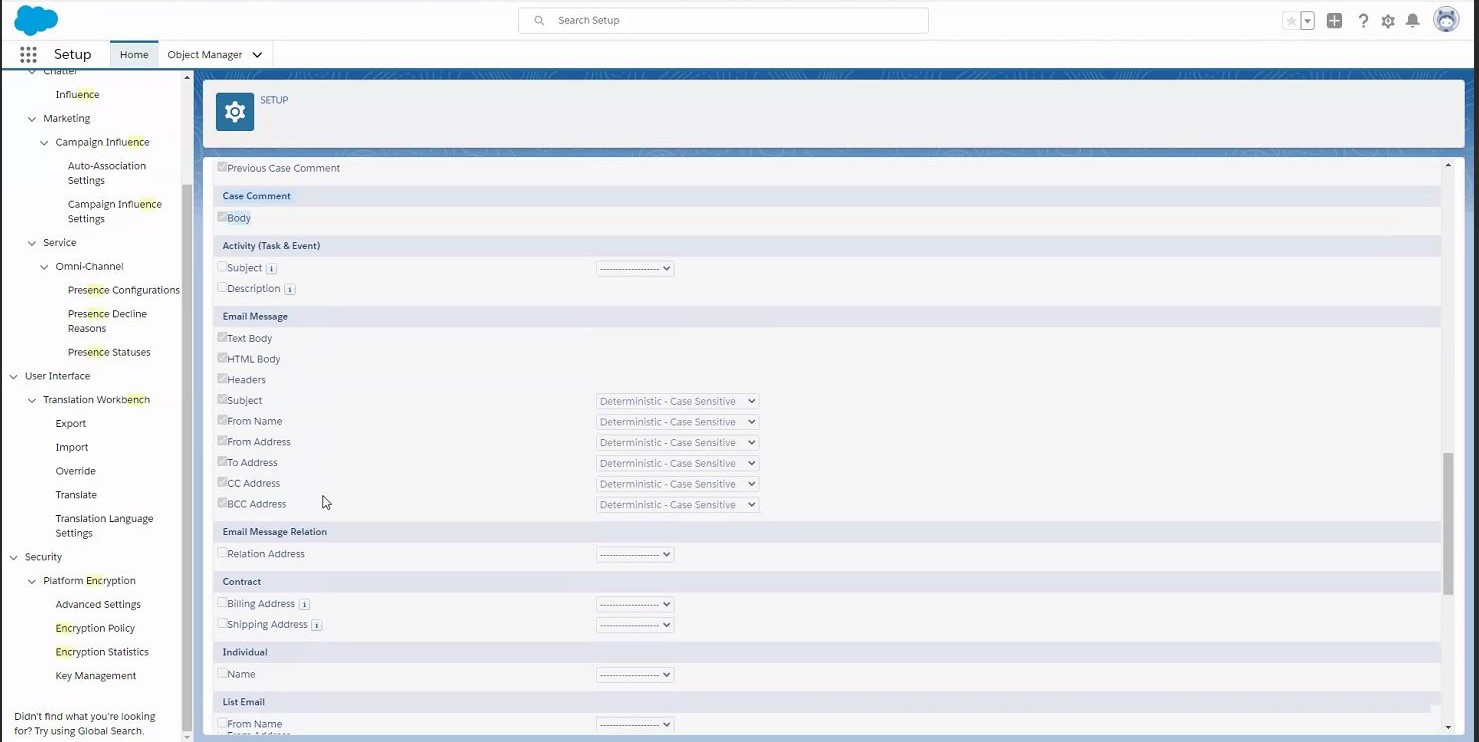


List 3: Screenshot showing potential sensitive information pulled out of the transaction log

D2.3

During client meeting, IA obtained screenshots of development team user interface showcasing encryption standard fields. IA observed in the screenshot, personal information and other relatively sensitive data is encrypted at rest. Likewise, the personnel that provided access to this information has the appropriate authorization to generate these data.





List 4: Screenshot showing potential sensitive information is secured and encrypted at rest