share one

NSHome and NSMobile Reporting Suite

During the COVID-19 pandemic, credit unions are seeing an increasing number of members utilizing their online services. With increased utilization comes an increase of potential fraud and subpoenas from authoriries requesting information for active cases of identity theft. This has been especially true over the past couple of weeks. Multiple clients have requested login data and activity from members' accounts who have reported fraudulent activity either to the credit union or to authorities. Share One has compiled a list of six NSQuery reports to assist in gathering this information. Along with the SecureAuth visualization reports located in the NSReport section of the Customer Portal, clients can run these reports to supply data in an easy-to-read format as needed.

An important reminder when using these reports alongside our SecureAuth visualization suite is the use of the Master ID field. In accordance with the General Data Privacy Regulation (GDPR), the member's account number is not used. Instead, the Master ID is used as a secure identifier as it does not reveal any private information about the member, such as name, age, date of birth, address, account number, etc. Depending on where you start with your research for the member, you may need to use the Master ID within NewSolutions if the account number is not on-hand. These reports are designed to allow users to enter either account numbers or Master IDs on the same report, cutting down the need for two separate report configurations for the same results.

Below is a list of the reports provided in the NSQuery reporting suite. All of the reports are set up in a way that the users can enter in a single account/Master ID or a list of accounts/Master IDs to retrieve multiple members on the same report.

- Member Lookup by Master ID – When reviewing information on the SecureAuth Dashboards, users may need to locate an account number by the Master ID. This report prompts users to enter the Master ID and produces the corresponding account number.
- Member Lookup by Account – Going the opposite route, when wanting to utilize the SecureAuth Dashboards, users must use a member's Master ID to retrieve information. This report prompts users to enter the account number and produces the corresponding Master ID.
- NSHome Login Tracking – Tracks the logins to NSHome via the website. Indicates if the member logged in from a PC or from a mobile device via the website (not the NSMobile App) and lists device/browser information and IP Addresses.
- NSMobile Login Tracking – Tracks the logins to NSMobile via the app. Displays device information and IP Address. Does not report logins from the website/browser regardless of what device was used.
- Member Home and Mobile Banking Profile – Lists dates for the last login, last login attempt, last password change, member's username, etc. for an entered account. This is most of the information displayed under EFT Access in Teller.
- Member Transactions via Home and Mobile Banking – Displays any transaction performed on a member's account by the NS3User. As a reminder, this user signifies transactions performed by the member via NSHome or NSMobile.

These reports have been uploaded to all Hosted and Service Center clients and can be found under the NSQuery folder labeled NSHome and NSMobile Reports. For In-House clients, the downloaded zip file can be found on the SSC under Featured Downloads. If you have any questions, please feel free to contact Bobby Rowland at browland@shareone.com.