**\*Summary\***

To the fraud team, MVP for direct deposit metrics is the first three items in the list they sent us. Those items are:

- IP Address of individual accessing record (including attributes about the IP, such as

geolocation coordinates, location titles, etc.)

- \*Note\*: They can do without geolocation for MVP

- Need within 8 hours of a subpoena from DoJ

- Authentication steps taken (with UTC timestamps)

- Login and logout times (including timeouts)

- It is not an issue if people close their browser instead of logging out.

In terms of MVP features versus a more comprehensive set of metrics, the team said they would be willing to go without some features for \*up to 2 months\* since they consider 2FA to be a big win. But it does put them in a compromising position and they would absolutely need this information eventually.

We need to work with ID.me to figure out what is possible to get to the fraud team and in what timeline.

It seems there are issues with what info we can get from MHV. We need to check on this (as Kam mentioned).

**\*Next Steps\***

- Chris, David, and Samara to regroup internally on larger strategy with this project.

- David to work with MHV to figure out their capabilities.

- David and Kam to talk about IP address and tying it to login times.

Event log list is what they have right now and what they definitely need going forward.

* From eBenefits/DMDC or whatever (**bold** = MVP)
  + **IP Address of individual accessing record (including attributes about the IP, such as geolocation coordinates, location titles, etc.)**
  + **Authentication steps taken (with UTC timestamps)**
  + **Login and logout times (including timeouts)**
  + Email(s) used (in case of outbound emails)
  + Cellphone numbers used (in cases of outbound texts)
* From call center
  + Telephone number used to make inbound calls (if applicable)

David to Kam — what can we supply now:

* **We do not log IP address directly, but we could easily begin logging that for each inbound request that comes in**
* **Geolocation would be more difficult to do. We are using [a service] that does not have that capability available.**
* **Login/logout time**s — a user closing their browser does not trigger a logout even though the user is not using their account anymore.
  + Fraud team — This doesn’t matter. We just need the time between to know when an even occurs. We don’t expect that people will necessary log out (though criminals might).
* We have logs in a limited capacity, but we can add IP address.
* What about email address — We don’t specifically log anything that could be PII including email address. We do have the ID.me account/wallet ID in our logs, though. But we could use this to get an email address
  + Fraud team — **We need to get this in less than 8 hours in order to answer federal subpoenas.**
* Fraud team — We should check to see whether we’d still have access to IP addresses at DMDC.
  + David — You’ll still have this for those logging in with DS Logon.
* Fraud team — Confirmed we can move forward without geolocation.

Authentication steps

* Fraud team — Something about logging in and then knowing where they went. Need to know what pages they go to and from what IP address. This is all done via DMDC now.
  + David — Trying to understand authentication vs. audit log.
  + Fraud team — Right now, it is limited to where they authenticate.
  + David — How much more detailed do we need to get?
  + Fraud team — Failed ID protocol, update direct deposit (timestamp). That sound be enough to start.
  + David — How many steps up to authentication do you need? Something like password reset would be really complicated. Anything beyond the session is difficult.
  + Fraud team — That’s tough. Where it is really critical is prosecution. It’s not always about diverting a payment. It’s about stealing a person’s ID to access a federal system.
  + Fraud team — When we are doing cases, we are running many IPs and trying to find all activity for these IPs. We are looking for all the things the IP address used instead of just one user. Eg. IP address could have access hundreds of accounts.
* How do we get this info to the fraud team?
* More about password reset — everything passes through ID.me. From an MHV perspective, if someone resets the password on their side, ID.me and VA.gov won’t know that.
* Fraud team — Currently can see a lot of the authentication and logging information they’ve mentioned. All of this is used for models. They \*could\* get by without it but this would reduce their accuracy rate.
* David says MVP would not be where functionality stops. Trying to determine whether we can move forward with some sort of limited functionality for an MVP or whether that’s not possible.
* Fraud team — Moving to VA.gov is good for more security, but without logs, we are having to figure out how long will we have to postpone giving info to Department of Justice.
* Chris — Where is the line on timeline?
* Fraud team — If we lost them for a couple of months, they’d have to apologize a lot to DOJ.
* What we are talking about — Pre session stuff. Still have access to DS Logon users.
* We can go back to ID.me and ask them how long it would be able to take to turn around more detailed information. **The bigger concern is what kind of logging is happening with MHV**. So
  + DS Logon is already good to go
  + ID.me we can make happen in some amount of time
  + MHV is more of a concern.
* Chris — Do you get any data from MHV?
  + Fraud team — We haven’t worked with MHV really. Fraudsters are going to MHV, taking health info, and using that to hack eBenefits. But we don’t have to solve MHV problem. **If we have to go a couple months without info, we’d survive. I’d take that risk for 2FA**.
* David and Kam to talk about IP address and tying it to login times. David to also talk with ID.me about other asks.