Direct deposit call 6.5.19

* Jeremy: What are we capturing in logs?
  + ID.me: Every authentication is linked through ID.me regardless of what credential they use.
  + It sounds like they do track IP addresses on the ID.me side, but they don’t have a way for an external party to get that information
  + Potential solutions: Pass on information somehow to VA.gov team or take end user IP address for VA.gov to expose that information. This would probably have to be stored somewhere where can correlate that with actual login events.
  + All the pieces are there, the question is how this information can be consumed?
  + They have internal tools for fraud investigation. They don’t just collect login events, but also key events in the interaction. For a one off case, they could escalate it through their support team.
* Jeremy: We don’t do one-off investigations. Usually, they do “connected case analysis” and look for fraud rings and map what they do in the system. So, they aren’t singular, it’s more a table of events they need to be able to run analytics event and can track things over time.
* David: Jeremy — can you share what you need from the team?
  + Jeremy: We use call center logs, web ops, web traffic logs, CorpDB, what they changed in the system, DMDC logs (where we get IP address info). If we can still pull this stuff from DMDC, then it’s not a show stopper for June 2019. What we need to make sure is we have a digital footprint. They don’t need to be saved. We pull IP addresses as things happen. We’re looking for where the table sits with the **IP address and what they changed**.
* David: We are getting better at codifying login and session events…. [missed some] We need to make sure you have what you need and then the fraud team could also work directly with ID.me to get other info. It doesn’t sound like you need to plug in directly to ID.me, you should be able to pull into what VA.gov has.
* Tanel: Is there anything we can do to make sure investigation isn’t necessary?
  + Jeremy: One problem is the OPM leak and other leaks. We don’t have 2fA on eBenefits right now, which is why we are pushing for 2FA to stop the bleeding. But criminals are getting better. They are getting information from our system and then taking that info to the private sector.
* Pradheep: If user is currently using their DS Logon, if their account has already been authenticated at level 2… when they start accessing this on VA.gov, what if you ask them to go through more identity proofing?
  + **\*\*DS logon 2 needs to re-verify?**
* Jeremy: Concerns — security questions are weaker than passwords. When we are sending out verification, something about phone numbers and preventing forwarding… No security question on password reset. Our proofing never relies on knowledge based questions for verifying. People have to have some sort of government ID or verified device. If one of the major vectors is on proofing, then MFA won’t protect the account because if the account is taken over, the fraudster can set whatever they want for MFA. We can normalize some of this if we require all verification at LOA3. Essentially, we don’t want to be responsible for techniques that are vulnerable because we’ll continue to see fraud until we get knowledge out of the loop.
* ID.me: Something about ID.me packing up info and sending it to VA.gov. Also happy to share information with them.
* Jeremy: We have patchwork ways to make this work…
* ID.me: 1) Let us know what data you need and we can package that up for you. 2) If we have to accept DS logon proofing and proofing is the major vector for fraud, MFA isn’t going to help. We’re confident that if we turn on LOA3 with our measures in place, we can reduce fraud. [Mentions other fraud prevention].
* Sounds like ID.me and Jeremy are happy to work together to get this resolved.
* Follow up:
  + Jeremy to get what he’s getting from eBenefits/DMDC to see what ID.me needs to get him and to figure out the best way to do so.
  + Jeremy offered up putting together a user story on how they use this info and the best way to achieve this.
* Pradheep: Timeframe?
  + Jeremy: If we still have 2FA and IP addresses from DMDC, then we are good. If we don’t, then that’s when things become critical.

DSVA next steps:

* Confirm what Jeremy needs as a baseline
* VA.gov should have the login info that Jeremy needs… how do we get that to him?
* Are we storing info we could export out?
* Chris to follow up and find who C&P team is that we need to talk to.
* Samara to regroup with Nick and TJ.