Consumer Financial Protection Bureau

Taskforce on Federal Consumer Financial Law Listening Session

August 3, 2020
2:00pm to 3:00pm Eastern

Participants: Taskforce and Consumer Advisory Board Members

Taskforce Participants: Dr. Howard Beales

Taskforce Staff and CFPB Participants: Nat Weber – Staff Director, Ashlie Tarpley – Taskforce Senior Counsel, Alex Nongard – Taskforce Support Staff, Crystal Dully – Advisory Board and Councils Outreach Engagement Specialist

Consumer Advisory Board Participants: Sameh Elamawy – CEO of Scratch Services, John Erik Beguin – President/CEO of Austin Capital Bank, Doe Gregersen – VP/General Counsel at Landmark Credit Union, Heidi Sexton – EVP/COO of Sound Community Bank

Readout: On Monday August 3, 2020, Dr. Howard Beales, member of the Taskforce on Federal Consumer Financial Law (Taskforce), met remotely via WebEx with various members of the Bureau's Consumer Advisory Boards and Committees (CABC) as part of the Taskforce's commitment to engage with external subject matter experts and stakeholders to gain insights regarding the financial service industry and financial consumer protection laws. Specifically, the group discussed the manner in which personal information is used to deter, detect, and mitigate fraud and consumer responses to such use.

Crystal Dully welcomed the CABC members, and Nat Weber made opening remarks and introduced Dr. Howard Beales. Howard referenced the background reading material, an excerpt from a textbook he authored titled *Business Government Relations: An Economic Perspective*, 2nd edition, Kendall Hunt, 2012. The excerpt notes the deleterious effect of fraud on consumers and financial services providers. It also identifies account fraud as the most serious form of identity theft and fraud on an existing account as another way identity theft presents itself. Additionally, the excerpt notes that reducing identity theft may require more information sharing, e.g. data triangulation used to detect fraud.

Howard asked the group to explain how fraud detection tools used personal information to combat fraud.

Heidi Sexton noted that her institution has outsourced this activity entirely to a third-party vendor. The third party uses client/consumer data to authenticate information. None of the tools use information gathered from social media for fraud monitoring. Heidi noted that identity theft regulations require financial institutions to have these kinds of tools in place, but the banks also have an independent incentive to monitor conduct. The tool(s) used at Heidi's institution provides a quantitative risk score and uses certain thresholds to determine if the institution needs to contact consumers directly to complete the verification process. Risk scores are used to determine if data provided by the consumer is out of line with normal behaviors.

Doe Gregersen explained that her institution used risk scores for check deposits to determine the the risk of a check bouncing. She noted it was hard to determine what information third parties were using to make this determination or how third parties had come by the information. The institution determined certain information a third party used was incomplete and sometimes outdated. This issue affected the usability of risk ratings. Eventually, the institution turned this particular tool off. Doe noted that other tools at her institution perform functions similar to those Heidi noted. Some tools provide quantitative score; others give pass/fail feedback. If there is a high-risk indicator, the institution asks for more information to verify identity and investigate the issue. This manual verification process is conducted for transactions performed online and by phone.

Sameh Elamawy further explained that in the case of fraud disputes, e.g. a borrower alleging there is a fraudulent loan on his/her account (e.g. when a borrower notices an unfamiliar loan on his/her credit report), the institution attempts to match the consumer's data to data provided by the borrower to determine if the consumer is a victim of fraud. If the institution determines that the transaction was fraudulent, it can remove the transaction from the consumer's account. In a lot of cases, the institution is being asked to prove a negative, which is difficult. Additionally, it is difficult to prove the consumer did not complete the transaction if the data used on the application is accurate/matches the consumer's data. Sameh noted that his institution did not outsource fraud detection/mitigation, but the institution does use a variety of data and tools (e.g. skip tracing) during interactions with borrower. Some of these activities are performed internally (e.g. skip tracking) and some are outsourced (e.g. additional skip tracing provided by third parties). The institution uses a probability model with scoring between 0 and 100.

Howard Beguin commented that the fraud-related issues could be broken into one of three categories: 1) I.D. theft; 2) synthetic identity fraud; and 3) anti-fraud detection for new accts vs. transaction monitoring for existing accounts. Austin Capital Bank has a fintech division where the institution builds its own tools and other more traditional divisions that look at fraud as well. In the past, the institution has used social media to verify identity. Howard noted that the Social Security Administration (SSA) is debuting a new program, the electronic consent based Social Security Number Verification Service (eCBSV), that gives a binary yes or no result when provided with data such as name, address, tax ID, date of birth (all of which BSA/AML regulations require institutions to collect from its customers). The program will assist with combating identity fraud. Currently, credit repair mills encourage borrowers to call their institutions and claim they did not take out certain loans. The Fair Trade Commission's identity

theft report does not require borrowers to file consumer complaints prior to disputing loan transactions. So, consumers can dispute loans without providing any evidence. This practice puts the lender in difficult position because the lender has to figure out whether or not there is actual fraud. The institution uses other attributes or identification to verify information provided by the borrower. With respect to Dodd-Frank section 1033, Howard noted that transaction monitoring for fraud is a double edge sword – it can be good or bad for consumers. For example, Howard asked the group to consider a situation in which a bad actor gained access to consumer data via a service like Plaid and as a result gains access to transaction information on an account. Most bank AML monitoring would asks an institution to determine if a consumer's transaction is out of the ordinary. But if a bad actor has the consumer's transaction information, it can mimic account activity to defraud the consumer and institution. As a result, Howard expressed that he is both excited and nervous about Section 1033. Right now, Howard noted the issue presented in the example is not happening, but criminals may be excited about the theoretical opportunity the regulation could present to commit fraud.

Howard added that Mobile account openings account for 80% of Austin Capital's total account openings. The institution is currently looking into using video KYC and facial recognition algorithms to verify identity for account openings. Dr. Howard Beales asked whether racial bias in facial recognition was an issue that Austin Capital is considering as it determines whether to implement this function. Howard Beguin explained that manual approval would be used if the institution were unable to verify identity through facial recognition and manual approval would be blind as to race.

Dr. Howard Beales inquired about the specifics of the SSA eCBSV tool. Howard Beguin clarified that the program is in pilot and that the SSA is only beginning to make it available publicly. The program would positively match the name of the consumer to a social security number. Previously, institutions used Lexis Nexis and other services to triangulate information to try to match it to the consumer. Dr. Howard Beales noted that the Department of Homeland Security looked at e-verify for employment purposes, but that the SSA did not verify information in database until someone tried to claim social security. Dr. Howard Beales asked how the new SSA system would address this issue. Howard Beguin said he believed the database would only be accessible to banks or other financial institutions which might address the issue.

Howard Beguin ended his observations by suggesting there should be a national block on credit reporting for social security numbers belonging to individuals less than 18 years old. Howard said a number of individuals who turn 18 may discover that their social security number has been used for a number of years by other people. Howard observed that he is unaware of any reason why it would be necessary to report the credit of someone less than 18 years old or why institutions would allow someone to get credit for a consumer less than 18 years old. He suggested there should be an immediate flag that there should be no credit reporting for the consumer.

Nat Weber asked the group if there were any recommendations for the Bureau in the area of data security/data privacy and use of consumer data for verification. Dr. Howard Beales

followed up by asking the group how important secondary uses of information are in building and using anti-fraud tools. He provided the example of magazine subscriptions being used to verify identity by lining up addresses on the subscriptions with those provided by a consumer.

Doe Gregersen remarked that consumer data should be secured to the highest extent. She also noted that while interacting with a national mortgage company online, she only had to supply her address for the company to populate all her information (e.g. the company ran her credit without her having to provide her social security number, knew her husband's name, obtained her title information, etc.). In that situation, the information the mortgage company obtained may have been coming from a third-party, so the information would not be considered the mortgage company's data. Doe remarked that any guidance the Bureau issued with respect to institutions securing this data may be difficult to implement because the data would not belong to them and may be housed on a third-party's server or database. On the other hand, the consumer would see the institution as the face of the breach. Doe recommended that any security provisions implemented by the Bureau extend to vendors/third-parties that institutions contract with to perform the services.

Heidi Sexton shared an experience similar to Doe's and noted a company she had interacted with had obtained additional information about her after she provided her cellphone number.

Sameh Elamawy observed that he did not believe consumers were aware of or notified of all secondary uses of data especially in the case where the consumer's data was being used for retargeting. Sameh recommended that there be rules implemented regarding transparency and control of consumer data. He noted that it was difficult to determine primary and secondary uses of information, so consumers could only hope for control and transparency when feasible. Dr. Howard Beales commented that a number of secondary uses are not disclosed because they are not envisioned at the time the data is collected (e.g. traffic data making location available). Instead, he believed transparency is a means rather than an end. As an example, he noted that a new computer has thousands of programs on it and the consumer is ignorant of what each one does and the notion of there being a disclosure of what the programs do did not seem to address the real issue of preventing bad things from happening as a result of using data. Sameh agreed that consumers may have varying levels of awareness and familiarity with financial products/services. He presented PPP borrowers as an example. He noticed PPP borrowers ask specific questions that other borrowers typically do not.

Dr. Howard Beales asked whether vendors provide institutions with information about the kind of data they use for their tools.

Doe Gregersen observed that some vendors cite where information is coming from and a lot make a blanket statement noting that the information comes from public sources. A lot of companies buy information where ever they can but do not provide a list of where they are buying it. Doe also noted that some vendors have reciprocation requirements with institutions. Pursuant to those agreements, the institution uses the data in the database and provides

information to the vendor to augment the database. The vendor collects data from the institution as it uses the vendor's product/service.

Dr. Howard Beales asked whether consumers object to the use of their data for anti-fraud purposes, and if so, on what grounds they object.

Doe Gregersen commented that the consumers do not formulate objections in a manner that suggests they are opposed to the institution using their data for a purpose outside of that which it was originally collected. But this view could easily shift if people's rights and awareness were changed through laws like the General Data Protection Regulation and the California Consumer Privacy Act. Currently, institutions put data into a "pot" and use it for whatever purposes it wants or needs so long as it is line with laws like the Gramm-Leach-Bliley Act. Otherwise, there is not a lot of transparency regarding the purpose for which data is being used internally at an institution.

Howard followed up by asking whether consumers push back when an institution is unable to verify information through the original verification methods. Doe said pushback happens when the consumer sees the additional verification steps as an inconvenience. The consumer does not push back because the institution is using the consumer's information for verification.

Howard asked the group whether fair lending concerns played a role in their use of fraud alerts and whether institutions were testing fraud alerts to make sure they were not disproportionately affecting certain populations?

Doe Gregersen commented that her institution was concerned about making sure tools did not disproportionally affect certain populations. But she noted that her institution was unlikely to deny someone for a loan due to an identity mismatch or fraud alert because there was no automatic denial for lending. For account opening, the institution uses certain databases and hires a vendor who manages that data. If a person were unable to open an account due to the institution's inability to verify their identity, it would be difficult to know the person's race because the institution would not have an established relationship with that person.

Howard asked the group if they had any sense of the number of false positives and false negatives they get from anti-fraud tools?

Doe Gregersen said she did not have the data on-hand but that the figures would vary depending on the anti-fraud tool the institution used and financial product. There is a different risk-rating scale for each of them.

Howard Beguin said he did not have these figures either but that the institution did monitor the application process for efficiency. He also noted that if there was a quantitative cutoff, then the risk-rating cutoff might affect the kind of fraud the institution saw. Howard said the institution might also see qualitative indicators of fraud.

Heidi Sexton commented that her institution analyzes risk thresholds to determine whether they needed to be lowered or increased.

Nat Weber, Dr. Howard Beales, and Crystal Dully ended the call by thanking the CABC members for their thoughtful responses and time. Nat Weber noted their information would be used to shed light on issues discussed in the first volume of the Taskforce Report.