CADWALADER

CABINET NEWS

Research and commentary on regulatory and other financial services topics

CFPB Report Concludes That GLBA and the FCRA Are Showing Their Age

November 14, 2024

By Mercedes Kelley Tunstall
Partner | Financial Regulation

On November 12, the Consumer Financial Protection Bureau ("CFPB") published a report called "State Consumer Privacy Laws and the Monetization of Consumer Financial Data" that took an uneven look at how Federal financial privacy laws fare compared to the comprehensive privacy laws that eighteen states have enacted in recent years. The financial services industry in the United States has had privacy laws dating back to 1970 (i.e., the Fair Credit Reporting Act ("FCRA") was passed in 1970) that govern how nonpublic personal information of a financial nature may and may not be accessed, collected, shared, and sold. Recent updates aside, the last major financial privacy law enacted was the Gramm-Leach-Bliley Act ("GLBA") in 1999, which was at the dawn of internet shopping and e-commerce. While there have definitely been updates to both GLBA and the FCRA and the various regulations that spawn from them, there has not been a new federal financial privacy law introduced in the past twenty-five years.

Meanwhile, the state privacy laws that have been passed, while comprehensive in nature (meaning that they address privacy rights and obligations generally and regardless of the sector in which the data is being collected or shared), nevertheless often exempt financial institutions regulated by GLBA. And, the CFPB thinks that this exemption may be improper and may leave many loopholes through which financial institutions may be able to drive trucks. To understand this, we are first going to look at what criticisms the CFPB has of the current laws, and then we will get into the sometimes fanciful conclusions the CFPB draws from them.

In the report, the CFPB points out that GLBA uses an opt-out mechanism, instead of a more privacy-protective opt-in mechanism. Specifically, when a financial institution governed by GLBA engages in the activity of sharing information with non-affiliated third parties, then customers have the right to "opt-out" of that kind of sharing. But, keep in mind that the opt-out process is cumbersome to operationalize because the opt-out has to be exercised only after the customer relationship has been formed, and then customers may either opt-out during an initial period of time or "a consumer may exercise the right to opt out at any time." 12 CFR § 1016.7(f)(5)(iii)(C), this is the CFPB's version of Regulation P, implementing GLBA. This means that in reality, almost all financial institutions governed by GLBA do not share information with non-affiliated third parties. So, this criticism seems to be a bit of a red herring.

Keeping in mind that the CFPB has had the ability to update its Regulation P (i.e., each federal banking agency and the Federal Trade Commission (FTC) have promulgated a separate Regulation P that is customized to address its regulated audience) since 2011 and has only put into place a few small changes, the report points out that there is no central repository for customers to indicate that they do not want their information shared, so they have to opt-out from EACH financial institution. Central repositories like the FTC's Do Not Call list have problems of their own, and again, because of the awkward nature of the GLBA opt-out, most financial institutions do not share information with non-affiliated third parties, so this criticism also seems to be swimming with the red fishes.

Finally, the CFPB points to the Government Accountability Office expressing "concerns that some financial institutions are abusing Regulation P's model notice option to mask just how much data they collect on consumers and all the ways they allow that information to be used, including by firms far removed from the products and services the financial institution provides." Why the CFPB itself does not have better information than the GAO about whether this kind of thing is actually happening is curious, given its supervision powers. But, more importantly, for anyone who has ever worked with the "model notice" required under Regulation P, the notice has been confusing since its inception. Yours truly has personally addressed this problem over and over again with the regulators, including with the CFPB and the FTC, and not only to no avail, but worse also to no real understanding from the regulators as to why the model notice just does not work. And yet, this is the one criticism of GLBA in the report that actually sticks.

We should now move to what the CFPB sees as being the big, bad result of the existing financial privacy laws – while recognizing that financial data includes transactional information, account numbers and such, the report also states

that “[f]inancial data can also include information that financial institutions compile using third-party products and services, such as a consumer’s credit score or a consumers’ web browsing history tracked through cookies, pixels, beacons, and related technology. Further, financial data can include the insights about a consumer’s behavior that their financial transactions reveal, such as details about what products and services consumers utilize, how much they are spending on these products and services, and where consumers are purchasing them.”

Never mind that the use of credit scores is highly regulated and restricted under the FCRA. Also, if a financial institution were to either use “insights about a consumer’s behavior” to make decisions about an individual consumer or to sell such insights so that others could make decisions about an individual consumer, then the financial institution would then have to comply with the FCRA in numerous additional ways, and if they get it wrong, then there is a private right of action under the FCRA. No, it seems that the biggest thing the CFPB doesn’t like is the possibility that financial institutions could use the data to create marketing profiles describing characteristics of broad swathes of consumers and make some money from that generic information.

So, what would the CFPB like instead? Obviously, the CFPB would like not just the generic swathes of data to be made available to anyone and everyone, but the CFPB have required financial institutions governed by GLBA to freely hand over all of the protected financial information to third-parties under their Open Banking Rule (read about that **here**), and all for free, and all regardless of whether those third parties or the consumers whose data will have to be shared are in any of the 18 states with comprehensive privacy laws. The new state laws do have some meaningful protections for consumers, but the main reason that those laws exempt financial institutions governed by GLBA is because financial services data is too complex for a generic privacy law to address responsibly, and money movement occurs across state lines in the blink of an eye. Only a new Federal financial privacy law would be appropriate to fill in whatever gaps, real or perceived, there might be, and in the meantime, it is relatively rare for laws to last as long as GLBA and the FCRA have lasted, and they have both stood the test of time.