Podcast: Data Privacy and Info Security in Finance: The Lay of the Land

February 08, 2023

In the age of big data, it's more important than ever to understand your obligations relating to your customers' private information. Information can be utilized by bad actors in a variety of ways that can be harmful to both you and your consumers.

Aaron Kouhoupt: Today we're going to talk a little bit about the privacy framework. I'm joined by my partner David Thompson, who is a Member of our Consumer Financial Services team located in our Cleveland office. Thanks for being with us today, David.

David Thompson: It's great to be here with you. Nice to talk to you.

Aaron Kouhoupt: I'm Aaron Kouhoupt. I'm also a Member in the Consumer Financial Services team, also located in Cleveland. I also have the privilege of serving as the firm's Chief Privacy Officer. So I get to deal with some of these things on a day-to-day basis. And I've spent a lot of my career in-house as the privacy officer at various entities, so I can feel everybody's pain when dealing with these privacy issues. So we're going to jump right.

You know, I think one of the things that's really important when we're thinking about privacy is to keep all of the different aspects of it straight, because there's multiple different things that we are thinking about. We're thinking about what is traditionally considered "information security": how you're keeping data safe and secure when you're transmitting it, when you're holding it on your servers, and just keeping that data safe.

There are also things that we're thinking about as it relates to what you can do with data that's in your possession, who you can share it with, what you can internally do with that data – really things around the usage and sharing of it. And then there's sort of this third area that is often forgotten about, really. And that is when a government agency comes knocking and says that they want information about your consumers, what are you supposed to do? How can you do that? It can be a little bit intimidating when you get that call or that letter from

an agency or the police saying, “we need information on your customer.” How are you supposed to react to that? And so those are the three major areas that you’re thinking about when we’re talking about privacy.

It’s not enough to know your own business model. You have to compare what you do with the activities that are permitted to bank and bank holding company subs.

There are both federal and state laws that are going to govern each of those things, and understanding where the overlay is and how they play together can be really important. On the federal side, the primary law that we’re thinking about is the Gramm Leach Bliley Act (GLBA). The Gramm Leach Bliley Act is going to govern both the data usage sharing issues we talked about, and it’s going to cover information security.

David, the one thing that I know you and I have talked about a lot and is something that needs to be really carefully considered is the definition of a financial institution, right? The Gramm Leach Bliley Act is going to govern financial institutions and that is a really broad definition, correct?

David Thompson: Gramm Leach Bliley, in this case, is implemented by Regulation P (Reg P), and Reg P is the starting point for my analysis of these things. The statute and the Reg both confirm that “financial institution” is defined much more broadly than you would think. And it kind of maps back to whether the parties are engaged in a business in which a subsidiary of a bank holding company could engage. So you end up in this situation where it’s not enough to know your own business model. You have to compare what you do with the activities that are permitted to bank and bank holding company subs, which is kind of a foreign concept. But there are lots of entities engaged in a business activity that’s technically allowed or contemplated by the bank regulatory structure. So we end up in a place where lots of clients who never consider themselves to be “financial institutions” find out, under Gramm Leach and Reg P, they are. So yes, it is broadly defined.

Am I governed by the Gramm Leach Bliley Act because I’m a financial institution? If I’m not, am I governed by these state laws that are there to, in a way, pick up where the Gramm Leach Bliley Act leaves off in protecting that data and giving consumers rights over data?

Aaron Kouhoupt: And that can get really interesting, especially because you know, where we’ve seen a lot of movement over the last couple of years is really on the state level. We’ve found a lot of states to have instituted privacy laws that are really geared primarily towards the, you know, usage and sharing of data. But interestingly, most, and we’ll talk about the one caveat here in a minute, but most of the states exempt financial institutions that are governed by the Gramm Leach Bliley Act. And so, the definition becomes that much more important, because now we’re thinking, okay, am I governed by the Gramm Leach Bliley Act because I’m a financial institution? If I’m not, am I governed by these state laws that are there to, in a way, pick up where the Gramm Leach Bliley Act leaves off in protecting that data and giving consumers rights over data? But the definition really becomes important if you’re trying to figure that out. And to your point, you may have thought you were not a financial institution, or maybe thought you *were* a financial institution. And now you really have to think about that from both directions, because you don’t want to find yourself on the wrong side of a state law because you’re not really a financial institution, and therefore you’re governed by these state laws.

David Thompson: I think it is becoming very important to go through the classification steps that you’re talking about. You have to understand not only entity type but information type. And so the thoughtful analysis of

Gramm Leach – your first question relates to whether you're engaged in activities that make you a financial institution, which technically maps back to are you providing financial products and services to individuals for personal, family, or household purposes. That's just sort of the general framework. You can be a financial institution or a service provider to a financial institution. Under both classifications you end up having duties that attach to how you get to use the data or how you're allowed to disclose it. So the evolution that you're talking about, Aaron, at the state level is interesting. Like in many cases, it gets started with California, who had perhaps a different goal in mind than many of us would expect.

They created a broader scope privacy law. It's not limited to financial privacy and financial institutions and consumers who get financial products. It's broader in scope and they do have an exception that hasn't been copied in the other states enacting similar laws, exactly. But they all contemplate either exceptions that are based on entity type (are you a financial institution) or information type, meaning is it non-public personal information or personally identifiable financial information? Because those are magic words under Gramm Leach and Reg P. So the evolving state privacy laws, a lot of them that create those exceptions, they point to whether the data in question is subject to the Gramm Leach Bliley Act and Reg P and they carve it out. And that can be really critical for a financial institution.

They all contemplate either exceptions that are based on entity type (are you a financial institution) or information type, meaning is it non-public personal information or personally identifiable financial information? Because those are magic words under Gramm Leach and Reg P.

But, Aaron, I know we've had lots of clients who have struggled with, if I'm a financial institution and the information that I receive and use and disclose is about people who are my consumers, they ask for a financial product or they get it. Do I have to care about the state privacy law that's just been enacted? And I think we have lots of clients who end up having to answer the question, yes. And it's usually because not everyone that you interact with is automatically your consumer or your customer, and whatever data you collect about those people before their data becomes protected by Gramm Leach is within the scope of a state law. So have you seen clients who've sort of struggled with a question of, how much do I care about the state privacy law and how do the pieces fit together?

Aaron Kouhoupt: Yeah, and I'm glad you talked about California because California created a little bit of an outlier scenario that, so far, the other states have not really followed. And what California did is exactly what you said, California did not give a blanket exemption to financial institutions. What they did is they exempted data that is subject to or pursuant to the Gramm Leach Bliley Act. And so what you find is this very odd spot where, even if you're a financial institution, you may have data that is not Gramm Leach Bliley covered information. It could be an IP address because you're tracking the way somebody's moving, certain cookies that are on the website that you have. And now you're almost in this data mapping exercise to say, here is all of the data I have and here is the data that is financial and covered by the Gramm Leach. Here is data that I don't really have that argument or it's questionable. And so I now have this California overlay.

The other states have so far, you know, they tackled it differently and they've exempted financial institutions at an entity level. It'll be interesting because there are a lot of states out there that still have bills pending, that are thinking about bills, to see if they sort of track the Virginia and the Connecticut and the Utah, who have gone to

the entity level to make that a little bit of an easier discussion. But in California, you know, our clients definitely struggle with that data mapping exercise. Oftentimes it's hard to say whether a particular piece of data is going to map to the Gramm Leach Bliley Act, or if it's going to kind of fall out and map to the state law.

California did not give a blanket exemption to financial institutions. What they did is they exempted data that is subject to or pursuant to the Gramm Leach Bliley Act.

David Thompson: So the other thing that makes California particularly nuanced and complicated is, over the years they've enacted a series of laws that implicate privacy. The counterpart to Gramm Leach and Reg P in California, which has been on the books for 20 years or more now, is the California Financial Information Privacy Act. That gets called out as well within the recently enacted law, the CCPA, CPRA, the Consumer Privacy Rights Act as it's now known. So I think people sometimes forget just how many privacy laws have been enacted by California. And they really have to sort of think through the process of how did you obtain the data, how does it get used, how does it get disclosed? And you're right, the data mapping exercise becomes pretty critical. And it's not just the California laws. The California residents essentially have protections that go above and beyond the federal privacy protections that exist, and that can depend on the context: whether it's financial data or health information or any other segment specific data that gets protected at the federal level. California in a sense goes above and beyond, having enacted a bunch of laws that add to the privacy complications and nuances that you find at the federal level. So, personally, I always have to do a back-check in California, just to run through the checklist of all the laws that have been enacted to take into account the possibility that I've covered all the bases, because there are so many that have been enacted at so many different times. It's a little bit of a struggle to keep them all straight, and our clients struggle with that too.

Aaron Kouhoupt: Yeah. To go back to where we started, you're also thinking about information security, and that can sometimes live in a different area of the entity. Oftentimes it's an area within IT, as opposed to legal, with some legal oversight over it. But you know, that's all the thing. We have seen some changes there with the FTC (Federal Trade Commission) safeguarding rule, about what an information security program should look like, and the things that you have to do in order to have a properly secure system, which includes encrypting data, it includes risk assessments, it includes reporting to the board. It's really just all of those things that frankly when I was in-house, I happily looked to my IT folks to understand system vulnerabilities and how they're going to keep everybody's data safe. And you have state overlay of those as well, including some states, like Illinois, who have biometric laws that require you to handle any sort of biometrics that you receive from a consumer with even more care.

You're also thinking about information security, and that can sometimes live in a different area of the entity. Oftentimes it's an area within IT, as opposed to legal.

You're also thinking about what happens in a data breach? In the unfortunate event that I have a data breach and I think that some consumer data was compromised, what do I need to do and who do I need to report to? And that's often going to map back to state law.

David Thompson: Yeah, you're exactly right. There are, for banks that are regulated by prudential regulators, there might be a different analysis that implicates the federal laws that attach to federally insured depository institutions. But at the state level, I think we're now at 50 states of the 51 jurisdictions that have enacted the

security breach notification laws. It started with California and several years passed and then a number of states enacted what amounts to similar laws but not perfectly similar. There are differences and it is kind of a complicated exercise.

The area where you find the most modifications to the previously enacted laws a lot of times has to do with what's deemed to be the "protected information." So you will find a law that gets enacted that defines the data points that might trigger the need for a security breach notification. And there's an ever-growing definition. It changes and expands over time to take into account email addresses or other things that you perhaps didn't think of as particularly sensitive data. It can be enough to trigger a security breach notification now.

On the cybersecurity front, I think the two states that have enacted laws that get the most attention from our clients are in New York and Massachusetts. Those essentially set a groundwork that require standards that go above and beyond, which you find expressly written at the federal level on subjects like encryption and secure transmissions. So as is often the case, if you have a client who's got a multi-state operation and they do business in a state like New York or Massachusetts, they end up having to create a compliance environment for the one state that's enacted the most stringent law, which in effect creates some safe harbors for them from other states that haven't yet enacted the law, but might treat a violation as a trade practice problem.

UDAAP is an area where there's really a lot of risk. There's just entities that might not quite fit neatly into one box or the other.

Aaron Kouhoupt: Yeah, and thank you, that's a great transition to the final point I wanted to talk about, which is impossible right now to ignore: UDAAP (Unfair and Discriminatory Acts and Practices Act) and unfair trade practices, especially where the Consumer Financial Protection Bureau (CFPB) has been very active in expanding, or maybe resurrecting as opposed to expanding, their UDAAP authority. And you know, UDAAP is an area where there's really a lot of risk, because even if one of these state laws doesn't apply to you directly, or even if there is an argument that that state law is not quite covering what I'm talking about, it's the conversations we had earlier where there's just entities that might not quite fit neatly into one box or the other. There is always this risk of the CFPB, thinking about the data sharing, in particular, practices as being unfair or abusive to the consumer.

And so it's not a bad idea to look at the way that you have your privacy program and your information security program set up, just to sort of level-set yourself against that risk and think about it a little bit as to, am I doing the most protected thing I can with the consumer's data? Does the consumer understand what I'm doing with my data? Am I being clear with my practices to the consumer? Because I think it's really hard to ignore that aggressive stance that the CFPB has taken.

David Thompson: I think you're right. And I think the other area that maps to financial privacy, but in a sort of a specific context, don't forget about the implications of the Fair Credit Reporting Act. You have a traditional credit bureaus, consumer reporting agencies, who have known for many years where they fit into the structure. They acquire information from data furnishers and then they are allowed, when they have a permissible purpose, to give it to a downstream user. You have a lot of intermediaries now who grab data in different ways. Then you have to figure out the definition of "consumer report" and "consumer reporting agency." Those are mutually dependent definitions. We keep encountering scenarios where parties claim not to be a consumer

reporting agency, but in effect what they're doing is grabbing data and selling it to downstream users, who are using it in a way that, together, forces the outcome that they didn't want. You inadvertently have the furnisher supplying data to an intermediary who gives it to someone else, and it makes them a consumer reporting agency, because they're not policing how the data gets used carefully when they give it to other parties.

You have a lot of intermediaries now who grab data in different ways. Then you have to figure out the definition of "consumer report" and "consumer reporting agency." Those are mutually dependent definitions.

Aaron Kouhoupt: Exactly. You know, we're running out of time. We've really articulated that there is a lot to be thinking about when you're thinking about privacy and people are not being shy. The states clearly care about this. We have new laws being enacted all the time, new laws being proposed. It's not something that people are ignoring. And I think that's only going to get more prevalent as time goes on, as we see all of these different news stories about both data breaches and just how much our houses are listening to us, right? I mean, going on to your phone after having a conversation and eight of the ads that you see are based on the conversation you just had. You're going to see a continued emphasis in this area. And especially if you're a financial institution or in the financial services space, you really need to be thinking about all of these different interplays and all of these different privacy laws. And there's no reason to be intimidated by them. You just have to slow down a little bit and look at each one and see where it applies to you.

So we appreciate all of your time. Thank you for joining me today, David, and talking about this, and we'll talk to you again soon.

David Thompson: Thank you.

download transcript

get more episodes

Subscribe wherever you listen to podcasts:

Related people

Aaron P. Kouhoupt

David W. Thompson