***The Consumer Finance Podcast* x *Payments Pros* –** Point-of-Sale Finance Series: Privacy, Breaches, and Data Monetization
Host: Taylor Gess
Guest: Kim Phan
Air Date: February 19, 2026

Taylor Gess (00:05):

Welcome to this special edition of *The Consumer Finance Podcast* and *Payments Pros*. I'm Taylor Gess, an associate in Troutman Pepper Locke's Consumer Financial Services Regulatory Practice, and I'll be your guest host for today's episode. Today we're going to be giving you another installment of our special highlight series on point-of-sale finance, where we discuss issues related to privacy and data security. But before we jump into that topic, let me remind you to visit and subscribe to our blogs, TroutmanFinancialServices.com and troutmanConsumerFinancialServicesLawMonitor.com. And don't forget about all of our other podcasts. We have the *FCRA Focus*, all about credit reporting, *The Crypto Exchange* about crypto and digital assets. We have *Unauthorized Access*, which is our privacy and data security podcast, and of course *Moving the Metal*, our auto finance podcast. All of those are available on all popular podcast platforms. Speaking of those platforms, if you like this podcast, please let us know. Leave us a review on your podcast platform of choice and tell us how we're doing. Now, as I said, today's episode is another in our special highlight series on point-of-sale finance. Here I'm joined by my colleague Kim Phan to give us some insights into privacy and data security. Welcome to the podcast, Kim.

Kim Phan (01:14):

Thanks for having me, Taylor. And I would be remiss in not noting that the firm also makes available Consumer Financial Services Privacy and Data Security Tracker. It is a service by which we provide weekly updates about all things in the world of privacy and data security related to consumer financial services. And we even have a monthly roundtable where we bring together all of our subscribers to chat about developments from the prior month and talk about trends and other points of interest. So if anyone's interested in that, feel free to reach out to me. But I'm thrilled to be here today to talk about this issue. Point-of-sale obviously is an area of great interest for both data security and privacy considerations. I was taking a look online a little bit before this conversation, and I saw a statistic that over 269 million payment cards were uploaded to the dark web in 2024. And obviously there will be at least some of those that were acquired from compromises at point-of-sale, whether or not physical points-of-sale at physical merchant locations or online through various e-commerce outlets. So, it's something that everyone should be thinking about.

Taylor Gess (02:26):

Yeah, that's a staggering number, Kim. It seems very large. Like you said, we hear a lot about data breaches these days. What should folks in point-of-sale finance keep in mind when it comes to data security and data breach in their practices?

Kim Phan (02:38):

One of the realities is, there's this increasing perspective amongst regulators that everyone in the chain of data is responsible for everyone else, either upstream to your bank clients, downstream to your merchants and their service providers, that there should be appropriate due diligence because any one of those points could be the nexus for a data breach. Right? You could have a skimmer that's onboarded onto a physical device at the merchant location. You could have keylogger malware that's uploaded to an e-commerce site that captures keystrokes of someone entering in their payment information. There's just a ton of points of potential vulnerability that could result in a data breach.

Kim Phan (03:22):

And it's increasingly the obligation of everyone to do appropriate due diligence, do monitoring and auditing to make sure that data, wherever it's originating from and wherever it goes, is being protected from end-to-end, where it's entered by the consumer all the way to where it's processed and the payment received. It can be challenging, right? And the reality is who is responsible is constantly shifting, right? You could lay everything on the entity that actually experienced the breach. And there's various laws, including on the state level, about laying out who's responsible for what. Mostly it's a question of contract. And state laws will generally honor contractual agreements between parties about who's responsible in the event of a breach, who has to notify, who has to pay the cost of credit monitoring, who has to notify attorneys general.

Kim Phan (04:13):

But if it's not something that companies think about ahead of time, that's one of those areas where it can get pretty messy once you're in the heat of an actual incident. The reality is also that state data breach laws, while we would love to have those be static so we can know what our obligations are and be sure about how we should move forward, one of the things is that we have 54 different jurisdictions that now have various data breach notification laws, all 50 states, Puerto Rico, the Virgin Islands, D.C., and Guam, as well as additional layers of obligations that fall on the financial sector, like the FTC's recent GLBA data breach notification rule, as well as for those entities that are publicly traded, some of the new SEC disclosure requirements. So, it gets complicated really fast. And not having a good incident response planning and preparation ahead of time makes it very difficult, especially in the area of point-of-sale where there are just so many parties involved. Right? The merchant, the equipment provider, the network provider, the payment processor, the acquiring bank, the merchant bank. You know there's... Just everybody in the world could be touched by something like that.

Taylor Gess (05:25):

Yeah, Kim, that makes a lot of sense. So when you're talking about these various different players that become involved in the point-of-sale finance space, what should all of our listeners keep in mind when it comes to vendor management and merchant oversight and those types of expectations that need to be had? I know those are especially crucial in point-of-sale.

Kim Phan (05:43):

Yeah, in the point-of-sale world, one of the things that always strikes me, and this is self-regulatory, not strictly a law, but I think we're all very familiar with PCI DSS, the Payment Card Industry Data Security Standards, which are issued by the Payment Card Security Council. It's a self-regulatory regime, but I hear over and over again from companies, whether or not the financial institutions or the retail merchants themselves, are like, oh, we have a payment processor who handles all that, so we don't have any obligations. And I'm like, no, that is incorrect. And vendor oversight is specifically the issue. What due diligence processes were in place when you were selecting your payment processor?

Kim Phan (06:24):

What contractual provisions did you ensure were in the written agreement with a payment processor who's going to be collecting, processing, and ultimately holding and someday disposing of that information all on your behalf because they are your service provider, as well as ongoing monitoring on auditing? All of that should be built into any sort of vendor oversight program. And it's always surprising to me for companies that may have very sophisticated vendor onboarding and oversight processes for many other types of vendors, point-of-sale vendors is often a blind spot for them because they just assume that they can use their payment processors and rely on them without having to do any further steps or investigations as to their own compliance obligations.

Taylor Gess (07:14):

Great. Thanks, Kim. So I know in privacy things are always changing. Right? Things are evolving and there's something new going on. Are there any new things on the state level that people should be following?

Kim Phan (07:27):

Well there's always stuff on the state level. Right. The federal government having taken a little bit of a step back from prior years when it was much more active in the payment space, like other areas of consumer protection, I think we're seeing something of a lull on the federal level. So a lot of the activity is very focused on the states. Some of it is not specific to point-of-sale finance. Right. These are laws of general applicability that may or may not apply into the point-of-sale environment. One of the big examples is, many of the new state comprehensive privacy laws, which are purportedly addressing every business that has personal information of state residents, often will have carve-outs or exceptions for payment processing and other consumer financial services under the federal Gramm-Leach-Bliley Act. Those exemptions come in two flavors. One is an entity-level exemption. So if you are a financial institution, which most point-of-sale payment processors, financing entities, and others are generally going to be exempt under those laws. But they always have to keep an eye on those few states that have limited GLBA data-level exemptions.

Kim Phan (08:44):

Those exemptions typically say if you are doing something that is specifically subject to the Gramm-Leach-Bliley Act, like processing a payment, generally that's going to be exempt. But there's a risk in those states because if you are doing anything further with the data, such as selling that data, using that data for marketing, that poses a risk that it falls outside of the GLBA and those state laws would be triggered. The states I'm thinking of are California. California is always going to be a concern in the regulatory world. Oregon, Minnesota, and that law just went into effect earlier this year on January 1st. But we have additional states that are also tweaking their GLBA exemptions, converting from that entity-level exemption, which is a very useful broad-based exemption, to the more limited data-level exemption.

Kim Phan (09:37):

There were two states last year that amended their state privacy laws to limit their GLBA exemption, and that was Connecticut and Montana. Connecticut, not surprising. Montana, not usually thinking of them as at the forefront of consumer protection. It is something that every state is paying attention to and it's pretty bipartisan. It's not really a Democrat or Republican issue. Everyone I think appreciates that if you have consumer financial information, that's very sensitive information and should be protected. So there's a lot happening from a state perspective with regard to privacy and this type of data, financial transactional data, what someone buys, where they buy it, how they're paying for it, whether a credit card or a debit card, EBT card, all of that has a lot of value in the world of data monetization these days.

Taylor Gess (10:33):

Yeah, Kim, so speaking of that monetization aspect, as we're wrapping up this podcast, do you want to tell us a little bit more about that and any other hot topics that you want to leave our listeners with?

Kim Phan (10:44):

Yeah, data monetization is certainly something I think most companies are at least exploring at this stage. I mean, there are some companies that have very simplistic processes. You know, this is all we do, and this is all we plan to do. But there are increasingly companies exploring, you know, we have all this data. Are there things that we can be doing with that data? And one of those is, can we be selling this data? Are there ways that we can get value out of this data other than purely operational? Right? So that's something that companies need to be thinking about. Whether or not data that is made available to that variety of participants that we mentioned being in the point-of-sale ecosystem, whether or not any one of those entities that may have access to this data can reuse that data in any way, can redisclose that data in any way, whether or not they can sell that data, that's an area that I think data monetization often will lead to. Can we sell this as a package deal? And if you do decide to start selling some of this data, and I'm thinking of some of the payment processors who have clients in every different industry. Right?

Kim Phan (11:54):

So, they're getting really high-quality data from a lot of different industries and looking at whether or not they can package that and resell it. One thing I would say for those folks is to keep an eye out for the Fair Credit Reporting Act. The FCRA being what, 55-plus years old now, like a very old statute, but it raises its head in so many different places that you always have to be keeping an eye out for it. Is your repackaging, your assembly and evaluation of that data and sale of that to third parties, does that become something that looks like a consumer report? Does that then make you, the entity who have compiled this information and sold it, a consumer reporting agency? And does that mean every other entity in that chain of data that we talked about earlier, does that make them furnishers of information? It is the reality of the FCRA that if any one entity becomes subject to the CRA as a consumer reporting agency, then they all sort of get pulled in and it's something to keep an eye on. And, there are some ways to mitigate that, right? You could have very clear contractual language that says, look, you can't reuse, redisclose, sell, or do anything else with our data.

Kim Phan (13:09):

But unless you have a clear prohibition like that in your contracts, you want to be keeping an eye on the partners that you are working with in the financial ecosystem, see what they're working on, what they're exploring. And, you know, I've seen this in a number of new pieces of legislation with regard specifically to the idea of data sales, this question of downstream recipients. If someone receives information, and even if your contract prohibits them from things like reselling that information, what are you doing to validate that? Are you auditing and confirming that they are complying with the provisions that you've laid out in that contract? I think that would be difficult for many companies that are involved in the point-of-sale ecosystem to audit up and downstream everyone who might touch that data. But I think it's becoming increasingly clear regulators have that expectation. I just don't know practically how companies will be able to do that effectively or at all in a way that would document this compliance with not a clear express regulatory obligation, but a regulatory expectation that we're hearing more and more from various government entities.

Taylor Gess (14:20):

Well, thank you, Kim, for being here with us today. I really appreciated getting to speak with you. We've done a great job highlighting some key privacy and data security issues for people in the point-of-sale finance space to consider. So let's leave this special series here for now and we'll pick back up with another very interesting topic on our next special joint episode for *The Consumer Finance Podcast* and *Payments Pros* on this topic. In the meantime, thanks to our audience for listening today and don't forget to visit and subscribe to our blogs, TroutmanFinancialServices.com and ConsumerFinancialServicesLawMonitor.com. While you're at it, why not visit us on the web at Troutman.com and add yourself to our consumer financial services email list? That way we can send you copies of the alerts and advisories that we send out, as well as invitations to our industry-only webinars that we put on from time to time. And of course, stay tuned for a great new episode of this podcast every Thursday afternoon and look forward to the remainder of our special highlight series on point-of-sale finance coming soon to your podcast feed. Thank you all for listening.

DISCLAIMER: This transcript was generated using artificial intelligence technology and may contain inaccuracies or errors. The transcript is provided "as is," with no warranty as to the accuracy or reliability. Please listen to the podcast for complete and accurate content. You may contact us to ask questions or to provide feedback if you believe that something is inaccurately transcribed.