***Payments Pros – The Payments Law Podcast* — Under the Radar: DOJ's Data Security Rules and Their Impact on Payments Companies**
Host: Carlin McCrory
Guest: Pete Jeydel

Carlin McCrory:

Welcome to another episode of *Payments Pros*, a Troutman Pepper Locke Podcast, focusing on the highly regulated and ever-evolving payment processing industry. This podcast features insights from members of our FinTech and payments practice, as well as guest commentary from business leaders and regulatory experts in the payments industry. I'm Carlin McCrory, one of the hosts of the podcast.

Before we jump into today's episode, let me remind you to visit and subscribe to our blog, TroutmanFinancialServices.com, and don't forget to check out our other podcasts on Troutman.com/Podcasts. We have episodes that focus on trends that drive enforcement activity, digital assets, consumer financial services, and more. Make sure to subscribe to hear the latest episodes.

Today, I'm joined by my colleague, Pete Jeydel, to discuss the new Department of Justice Data Security program that took effect earlier this year in the implication of these DOJ rules on data protection for payments companies and financial institutions. Pete leads the firm's Sanction and Trade Controls Team and is part of the White-Collar Litigation and Investigations Practice. He advises clients on regulatory compliance, M&A transactions, government inquiries, internal investigations, self-disclosures, and represents them in enforcement actions. Pete, thanks so much for joining me today.

Pete Jeydel:

Hey, Carlin. Thanks for having me.

Carlin McCrory:

All right. let's just start this off. What is the DOJ data security program that we're discussing today?

Pete Jeydel:

I love to talk about this, because it's really not gotten very much attention. It's really flying under the radar. It's important for companies in the payment space and a lot of different industries to really be aware of what this is. We'll try to cut through a lot of the complexity and just provide a high-level overview of what it is. This data security program, it's administered by the National Security Division at DOJ, Department of Justice.

I think one of the reasons it's flown under the radar is that it really appeared quickly. This was a super-fast rulemaking over the course of last year. There was an executive order in February of 2024 that President Biden issued that kicked this off, and then a series of rulemakings over just a 10-month period last year. It's really, I wouldn't say rushed, but quick. Final rule came out in December. It took effect just about a month ago, six weeks ago, in April. DOJ has offered a 90-day leniency period. The rules are in effect, but there's a leniency period until July 8th for companies that are engaged in good faith efforts to come into compliance, to complete their compliance approach under these rules.

This is basically an acknowledgement by DOJ that this is new. It's complicated and it's a really big deal for some companies. For many companies, it's much less of a big deal, but they've offered this 90-day window. That is not to be taken as an excuse to hit the snooze button on this. These are national security rules. These DOJ prosecutors are raring to go with an aggressive enforcement approach. The Trump administration has made clear that this is something they're pursuing. This is a China-focused national security rule, so it is definitely important to make use of this period through the spring and early summer to get that compliance approach ramped up and in good shape.

I mean, you're seeing a lot of brand-new regulatory regimes cropping up in recent years. You've got traditional export controls and sanctions. Now, you've got in the same space, you've got this DOJ data security program, you've got the BIS Commerce Department ICTS rules, you've got the new, people call reverse CFIUS, outbound investment security. These brand-new, really significant regulatory regimes, it's pretty overwhelming for a lot of companies. Hopefully, we can give listeners here a few minutes of an overview to really understand at a high level what's going on, and how this may impact them.

Carlin McCrory:

Yeah. It sounds like, from what you said, Pete, to highlight, that while many areas in the Trump administration, especially as it relates to the CFPB, we're seeing rules being pulled back where this is the opposite, and the Trump administration is actually saying they're going to enforce this and make it a priority. Do you have any thoughts on why the process perhaps, was so rushed and happened so quickly?

Pete Jeydel:

Yeah. I think the DOJ got a green light to do this with that executive order from President Biden, and they've been very concerned about this for years. It's the section in the National Security Division that does CFIUS, National Security Foreign Investment Reviews. They've been seeing data concerns in the foreign investment space for decades, for many years, focused on China when Chinese companies are acquiring US companies with sensitive personal data. DOJ and the US government Treasury at CFIUS have been addressing that kind of a band-aid approach, case by case, through CFIUS reviews. DOJ's been saying for years, players across US government have been saying for years, we can't just be looking at this transaction by transaction. We have to have a regulatory program here.

They say, CFIUS has been shutting the back door, but we've left the front door wide open. That's one of the analogies that the policy makers have provided. This data security program,

it's in across the board, regulatory regime that's meant to shut that front door by protecting this sensitive personal data from countries of concern and entities linked to countries of concern, and that is China, Russia, the usual suspects of foreign adversaries as the government calls them.

Carlin McCrory:

Okay, so then let's get into what's really new about these DOJ rules. I mean, we all know payments companies and financial institutions are already required to protect customer and, or customer rather, and transaction data. Do these rules really change that picture?

Pete Jeydel:

Yeah, it does. It's an entirely new framework of data security. It's unlike any other regulation that applies under US law, or under as far as I'm aware, most foreign laws. Again, these are national security rules, so the foundational concepts of data privacy, like individual consent are irrelevant here. DOJ's and the policy makers have made an analogy to export controls. They say, companies can't just consent to allowing their crown jewel technologies to be transferred to China, or other restricted countries without a license. They said, similarly, there's a public interest in this sensitive personal data, and we should not just allow people to consent to the broad-scale transfer of that sensitive personal data to our adversaries. There's a public interest in controlling that.

Similarly, other basic cornerstones of data privacy, like contractual protections, except in a few cases are irrelevant here. It's a really fundamentally different type of regulatory regime that applies here. The contractual provisions, DOJ has just seen through those niceties, and they said, look, the Chinese government could override those protections by invoking supremacy of local and national security laws, or just covertly by taking the data as they've done. It's an acknowledgement that aggressive state espionage has ramped up, and that we really need to have a clear-eyed regulatory approach that protects against that and acknowledges it.

Similarly, traditional data privacy, data masking techniques, other ways that companies can mitigate data privacy risk, generally not relevant here. DOJ has said, these rules apply, at least in the first instance, irrespective of any security measures, like encryption, de-identification, anonymization, and the like. It's really a fundamentally different framework. With respect to the data itself, there's a very different scope of what's covered data here. It's not necessarily your traditional PII categories, things like, criminal history, web browsing history, not covered here, not considered sensitive enough. US government, they like to say, their approach is, high-fence, small yard. We're not going to protect everything, but what falls within these regulatory areas, we're going to protect with some really stringent rules. Again, some major differences.

There is a law that was passed last year called PADFA, the Protecting Americans Data from Foreign Adversaries Act. A lot of people say, “Well, we already know how to comply with PADFA. It's all about China. Isn't it the same as these DOJ rules?” It's really not. PADFA is really quite different. There's a different scope of covered persons quite different. PADFA applies only to data brokers, whereas, the data security program is more activity-based based on any type of entity, or individual, can be subject to the data security program. Similarly, PADFA takes more of a traditional data privacy approach if an individual requests, or directs a

data transfer, then PADFA says, generally speaking, that's okay. Not going to be regulated. Whereas, again, DOJ doesn't allow for that type of consent in this national security context.

Carlin McCrory:

Pete, you mentioned at the top of the episode some companies will be greatly impacted and others not as much. Can you talk a little bit about what companies will be impacted by this?

Pete Jeydel:

Yeah. Maybe, I mean, it probably makes sense to step back for a second and just understand what these rules cover. They apply to sensitive personal data of US persons in their specific categories of data that fall within that, as well as certain types of US government related data, which is treated as being particularly sensitive. If you have these types of covered data linked to US persons and you have a country of concern, or an entity in a third country that's linked to a country of concern, like China or Russia, then these rules may apply. The companies that are primarily impacted by this, as far as my conversations and clients, I've been concerned, a lot of them are companies with Chinese ownership, for example. If they rely on the parent company, or vendors in China to carry out some of their essential functions and essentially require the data to be accessible within China, those companies are having a hugely difficult time complying here.

That whole construct is largely inconsistent with DOJ's objectives under these rules. We basically restrict the availability of this sensitive data in China. Essentially, any international company with covered data in its possession and its systems may have compliance obligations here. Those will vary based on the type of company, the exposure to the covered data, exposure to China, or other country of concern. I should say, even many purely domestic U.S.-based companies will have to take compliance steps under these rules. It is certainly focused on international data transfers, but, for example, DOJ is going to be publishing a list, basically, like a sanctions list called the covered persons list. They've said that may include U.S.-based entities, or even individuals that they have national security concerns about.

That may require companies to engage in a new type of, basically, a sanctions screening process, but with a really unique lens for these data security rules. The impact will vary quite a bit, but most companies, nearly all companies that have covered data, are going to have to worry about these rules, take steps to comply with these rules, again, during this 90-day leniency period that applies until July 8th.

Carlin McCrory:

That's really interesting, Pete, about perhaps, running a new sanctions screening basically, like many companies already have to do. Can we talk about the exemptions from the rule and how did those work?

Pete Jeydel:

Yeah. The DSP sets out some really harsh rules, quite intimidating for a lot of companies. The good news is the exemptions. There's a handful of exemptions. Some of them are quite broad. For this audience, I think probably most relevant is the financial services exemption. It is very broad, but it's not blanket. It's not a industry-wide across-the-board exemption. It applies to data access activities that are ordinarily incident to and part of the provision, or financial services.

The key language is ordinary. Is it ordinarily incident? Again, it's pretty broad, but it's not going to include all types of data access in China. If you have an odd, or unnecessary partnership with a Chinese company, or employee-based in China, the exemption is probably not going to apply. What I mean by odd, or unnecessary, it's not ordinary. For example, if that China connection is not related to the provision of a service in China, you're providing a service that is entirely within the United States among US persons, US merchants, US consumers, or between the US and the UK, or what have you. It has nothing to do with China. But you have an employee-based in China that needs to access data, because that's where you've found talent. You've got an employee there, or you have an investor who's based in China, who maybe sits on the board and has certain types of data access as part of the supervisory responsibility. That's odd. That's unusual. That's not ordinary for the provision of a service in the US, or outside of China.

In contrast, if you're providing a service in China, you may, for a variety of reasons, be essentially required to, or be quite ordinary to have localized data in China, work with Chinese partners, Chinese regulators, and the like. That's really what the exemptions meant to capture, activity that has a normal link to China, where Chinese partner, or would have you, is an ordinary feature of providing a service typically in China, where one of the parties is in China, or another country of concern. When that's the case, this exemption is actually quite broad. Bottom line, it's quite nuanced when it applies, but when it does apply, it's very broad.

The exemption lists a bunch of detailed types of financial services. It's an illustrative list. What is a financial service here? It includes payment processing, funds transfers. It also includes a bunch of ancillary services, like dispute resolution, fraud detection, things like that. Again, when the exemption applies, when the link to China is ordinary, the exemption is pretty broad.

Carlin McCrory:

What I'm gathering from this, Pete, is if a company that engages in financial services has a vendor with access to data and that vendor has a location in China with access to personal customer information, if it's ordinary, it is likely okay. Is that understanding correct?

Pete Jeydel:

That's basically it. Your tone and the way you've said that really highlights, there's a lot of gray area here. I mean, they literally use seven words. I'm counting the right, eight words, to capture the scope of this exemption. As you know, when you get into specific cases with clients, it's not going to be simple. Is this ordinarily incident to the provision of our service? There's a huge scope of gray area here. There's a lot of ways that you can tackle that. There is a formal advisory opinion process that DOJ has put in place and that will essentially open in July. That

basically said, please don't come in for the time being. But once the rules come into full effect, or the leniency period's over, they've said, sure, at that point, you can come in.

I suspect it's going to be a challenging process to get real clarity from DOJ and to get that the timely manner. I think companies shouldn't be overly optimistic about just leaning on DOJ. They're open for business. They will be in July, anyway. A lot of this comes down to the framework of these rules. The DSP is based on the authority of the International Emergency Economic Powers Act, IEPA. It's the same legal framework that applies under U.S. sanctions. It's the same national security division at DOJ. These are people who grew up with sanctions. Really, it's using good judgment to apply a risk-based compliance approach. These are national security division prosecutors. They're focused on real national security risk areas. They want companies, just like OFAC at Treasury, administering sanctions. They say, take a risk-based approach.

When you're thinking about, does this really ambiguous exemption apply? Think about why that exemption is there, the policy purpose for it, and how DOJ would likely construe it based on the national security policy that underlies this and a traditional IEPA risk-based compliance approach. Now, that sounds like a whole lot of jargon, but there's decades and decades of learning that goes behind that, that people can help companies to make good judgments here.

Now, that's not going to necessarily get you absolute clarity and certainty, unless you go into DOJ and get a written advisory opinion, so that for many companies, that's going to be the way they need to do this to get that certainty.

Carlin McCrory:

What are the penalties for non-compliance with this?

Pete Jeydel:

Yeah. It's an IEPA authority. It's essentially the same penalty framework that applies under sanctions. Civil penalties of inflation adjusted, it's like, 360 something per violation. Again, it's per violation. The government can define that in all kinds of ways. Each data, each event of access, we'll see how DOJ defines that. They've not been clear about that so far, but the expectation is that they'll readily seek to multiply those violations and get the penalty amounts up significantly. Civil penalties, or for willful conduct, criminal penalties, a million dollars per violation, 20 years imprisonment. Other rules will apply to the federal conspiracy statute and the like. Like sanctions, the penalties are really significant.

Again, I think what companies need to come back to is what's the starting point? How do we approach this initially? A lot of companies are really overwhelmed, confused by these rules. Again, it's starting with the basics. Understanding whether you have covered data in your systems and not to put in too much of a plug, but at Troutman, we've done a lot of work on this already. We've got off-the-shelf questionnaires that for our clients, we can send you these off-the-shelf materials to make this manageable, walk you through it really step by step to assess whether you have covered data. If you do, are your counterparties subject to these rules? We have questionnaires and flow charts that we can send that will really make this manageable for

companies that are really starting at the beginning, or reassessing their compliance approach here.

Then, at the end of the day, if when you get into the real tough areas, like the exemptions where it's gray. It's not black and white. There's a lot that we can do as outside council to help companies make these judgments. Again, what are the highest risk areas? These national security division prosecutors are not going to be looking to make cases based on minor technical missteps. They're going to be looking at the serious national security risks. That's going to be their priority.

Companies need to reflect that in their compliance approach. What are the real high-risk areas that our company is involved in? How would the government view it? Let's focus our compliance approach on these priority areas. I think with that type of framework, companies can go forward and develop a compliance approach that's going to work and that's going to satisfy DOJ.

Carlin McCrory:

All right. Pete, thank you so much for joining us today and thank you to our audience for listening to today's episode. Don't forget to visit our blog, TroutmanFinancialServices.com, and subscribe so you can get the latest updates. Please make sure to also subscribe to this podcast via Apple Podcast, Google Play, Stitcher, or whatever platform you use. We look forward to next time.

Pete Jeydel:

Thank you.