PAYMENTS PROS S02E10: TACKLING CREDIT PUSH FRAUD: UNDERSTANDING NACHA'S RISK MANAGEMENT PACKAGE

Keith Barnett: Welcome to another episode of Payments Pros, a Troutman Pepper, 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.

My name is Keith Barnett. I'm one of the hosts of the podcast. And before we jump into today's episode, let me remind you to visit and subscribe to our blog, troutmanpepperfinancialservices.com. And don't forget to check out our other podcasts on troutman.com/podcast. 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, Carlin and I are thrilled to welcome back Jordan Bennett. Nacha's Senior Director of Network Risk Management. This time, he's here for a special two-part series on the newly approved rules designed to combat credit push fraud.

By way of background, credit push fraud has been increasing in recent years. And in fact, Nacha released its risk management framework for the era of credit push fraud in late 2022. That release focused on increasing awareness of frauds using credit push payments such as business email comp compromise and other impersonations.

And last year, Jordan led our podcast by discussing that issue. And if you missed that podcast, please do not hesitate to go to it. It was on June 6th when we released that. And so, by way of background for today's episode, there are new rules approved by Nacha's members on March 18th, 2024. These rules aim to mitigate fraud incidents such as business email compromise, which I just discussed, and efforts to exploit credit push payments.

In the first part of this series, we'll explore the risk management package. There, we will discuss the comprehensive set of rules and multiple rule amendments that were included. The rule

amendments will be effective in October of this year. At least the first parts. And they are part of this larger risk management package that Jordan will discuss.

And without further ado, Jordan, it's great to have you back. And thank you for joining us to discuss these significant rule developments.

Jordan Bennett: Yeah. Thanks for having me on. I do want to point out that they do start – the effective dates do start at the end of this year for some. But some of them are all the way out into 2026. We do have some time for folks to prepare for these and to get ready.

And that last podcast we did, we talked about some RFCs that were out. Some requests for comment. And you'll see that most of what is in this package was in that – we discussed in that RFC. There are some changes. It took us quite some time to get this right. We wanted to make sure that as these amendments to the Nacha rules went out to balloting that they were exactly as they needed to be to help the network and to reduce the incidents of credit push frauds. And to give financial institutions useful tools. It's an excellent package that went out.

And then, of course, this update, we're not finished. The framework has there to guide us for the long term. Nacha is constantly updating the rules. Having RFCs, requests for comments. Putting out new ballots. We want to make sure that we are meeting the needs of the industry. And this is just one example of what we're doing to help the industry out.

Keith Barnett: No. Thanks. And that's helpful. Because one of the things that the industry has been talking about is exactly what you discussed, the risk management and payments. And so, in addition to what you just mentioned, is there anything else that Nacha is doing to address issues around payments fraud, especially around credit push fraud?

Jordan Bennett: Absolutely. We started out immediately with education. If you go to nacha.org/rmag, we have some risk management guidance out there. It's from a group of risk and compliance experts that get together and discuss things we should do for white papers, for guidance, for guidelines. And we put it out there and hope folks go to read it and then take some of that guidance and improve the risk and controls at their financial institution.

Many of the pieces are thought pieces to say – we don't necessarily tell you exactly what you need to do. But here are some considerations for this type of fraud. For this incident. How can you think about it and how can you help your financial institution protect yourself?

There's also pieces we've put out through different groups. Not just RMAG. But, yeah, just go around to the Nacha website and look for – explore that website. There's lots of good material out there.

Keith Barnett: That's great. And the other thing that is on the Nacha website are these new rules. And so, you'll have a lot of viewers on your website. And we also have quite a few listeners as well. For our listeners, could you briefly summarize the rules that were recently approved?

Jordan Bennett: Sure. The rules are really intended to fit together as a big package. They work together essentially as a team to kind of help us in the industry mitigate some of the effects of credit push fraud. The idea is to increase awareness of fraud schemes. Reduce the incidents of successful fraud attempts. And then improve recovery after frauds have occurred.

And so, with that, we've got an amendment for fraud monitoring by all parties in the ACH network, except for consumers. This is expanding traditional fraud monitoring from just the ODFI's for returns. Unauthorized, right? To include ODFI's looking at monitoring transactions that they're going out along with originators, third parties. And it includes the ODFI monitoring of inbound ACH credits.

And we also have new rules around fund recovery tools. We're changing the rules to allow an RDFI to return items for suspicious activity. We're clarifying the ODFI's ability to request a return. That's going to be much more broad in case there's a fraud scheme that has been identified by an originator or by the ODFI after it's been sent out. The ODFI can say, "Hey, I'd like to request that and get it back from the RDFI."

And there's also an exception to the RDFIs funds availability requirements. And that's going to line up with Reg CC. We want the RDFI to have as much time to pause a transaction, look at it and say, "Is this fraud or not?" And so, it lines up with other standards within the industry.

We're also standardizing certain data fields. The intro description for payroll and for purchase has been standardized. And we are trying to help the WSUD process. That's your Written Statement of Unauthorized Debit. We're changing the timeline a little bit there because payments and information have gotten so much faster. You can actually return an item if it's unauthorized as soon as that receiver is aware of it.

It used to be just on the settlement date or later. But, many times, the receiver knows of a transaction because it's either middle-of-posted or pre-posted before the actual settlement date. You don't have to wait until it hits that receiver's account to get that website anymore and to be within the Nacha rules.

And then we also want a prompt return of a debit after the receipt of a completed written statement. That timeline has sped up. And we know the faster that somebody responds to a fraud and lets the other parties know, the faster we can recover. That one is intended to increase the speed that the ODFI gets that run statement back. And so, I think you mentioned earlier the effective dates have a time frame of October 1st of this year through June 19th of 2026.

Keith Barnett: And so, one of the things you just mentioned were the fund recovery tools. Three of the amendments or enhancements. Two fund recovery tools. Could you explain to the audience how these tools can be used by the different parties?

Jordan Bennett: Absolutely. For funds recovery, we have allowing RDFIs to return for suspicious activity. And, previously, the Nacha rules have always stated that you can return an item for most any reason. You just have to find the right SEC code or the one that fits most closely.

And we are amending the rules to specifically state. RDFIs can return using an R17. And we're making the definition there, so it's much easier for an RDFI to return for suspicious activity. That allows an RDFI to say, "Hold on. This does not look right. We've done some monitoring. We think we have either a mule or we have a fraudster on our end. And we're going to return it." This is totally optional by the RDFI. It's not a mandatory thing that they have to do. But it is a tool that is available to them.

We also have the ODFIs ability to request a return. The reasons an ODFI could request a return previously were somewhat limited. And we now are stating that it's much more broad. And we've got a new term that we have defined. It is called false pretenses. And you're going to see a number of the new rules include references to this newly defined term.

And so, I do want to read you kind of the language there. False pretenses is the inducement of a payment by a person misrepresenting than a person's identity, that person's association with, or authority to act on behalf of another person, or the ownership of account to be credited. A number of these rules have that in there. And for that particular rule, you can return those if you find out – or you can ask for the return of the RDFI as an ODFI if you want to try and recover those funds after you identify what you think is a fraud.

And that last one is the exception to the RDFIs funds availability requirements. This exception is changing the Nacha rules to align with Reg CC. It doesn't go above and beyond that. You still have to give availability. But you have a little bit more time to do that research in cases of suspected fraud.

Carlin McCrory: Thanks, Jordan. And you also mentioned earlier a little bit about the standardization of information. What is the reasoning behind find these changes?

Jordan Bennett: The standardization here is – so an RDFI. If they choose to, as part of their monitoring, can put these terms into their algorithms or their tools to look for red flags. You would be absolutely surprised the number of ways you can say payroll. And for payroll misdirection fraud, if an RDFI can screen for one customer getting multiple payrolls when this is unusual, they can – if they're screening for one word as opposed to all of the different ways that

you can say payroll, it doesn't seem like there'd be a lot of ways. But there are. You can say payroll, you can say TPD payroll. You can say paycheck. I mean, different companies put their initials in front so you know that it's coming from this payroll provider. Or that it's coming from this employer. Standardizing that to one way is going to give those RDFIs who choose to look for that a much easier way to search and say, "Hold on. It looks like Carlin got four payrolls today. That doesn't seem right. Let me pause, and look, and see. Oh, wait. These are different names."

It's just one of those flags that can be used, right? It's not something that is going to be mandatory on the RDFI side. But it's just a flag that normally you receive, I'm sure, every week one dedicated payroll. And if you're tricked into becoming a mule or you're a fraudster and you start receiving a budget, that should be a flag to the RDFI.

Carlin McCrory: How can organizations adapt and use this information? I mean, you mentioned if I receive multiple payrolls, that's obviously a red flag. Are there other things and other ways organizations can use this information?

Jordan Bennett: You're talking about the standardization?

Carlin McCrory: Yes.

Jordan Bennett: Yeah. Anytime that you can make something more standard, it is easier. If you remember back in the original RFC podcast that we did, we had the name standard in there. And that didn't go through. We got a lot of feedback that it is extremely hard. Think of all the different ways you can say one person's name. And the fact that the ACH has been around for 50 years now, people have their patterns and their ways of doing things. And others thought it would lead to mandatory name matching, which is not what we're trying to do. But having a stand makes it much easier.

We are going to put the name standard into the guidelines. We're going to put out some guidance on standardizing a name, so RDFIs can see when something comes in as Carlin. Or if you have a joint account with your husband. Or people have – they go by different names,

nicknames, whatever. That can all kind of be worked through. But if something – if you, all of a sudden, get Keith into your account, that should be a red flag. Standardization of how that name can come in. And so, you see most of your names, or you see the payroll, or you see purchase and the entry description can really help RDFIs narrow down their search and really help their algorithms find these red flags that are going to be then brought up to a bank employee to investigate further.

Carlin McCrory: And the last thing I want to ask you about is you noted a group of changes surrounding WSUDs or those written statements of unauthorized debits, which are used for returning unauthorized debit payments. Why are these changes part of this package of amendments?

Jordan Bennett: Sure. We are always looking at ways to improve the rules. We are focused right now on credit push fraud. But that does not mean debit fraud has gone away. Right? We are trying to protect consumers and businesses from all types of fraud. And having these tools helps in the same way that some of the other credit push fraud amendments do. Right? We are trying to enhance the recovery of funds and to speed up that communication. The faster somebody can acknowledge that something is unauthorized and return that to the RDFI or the ODFI, the better.

And one thing I'd like to point out here is that all of your returns can go same day. And there's not a charge for that. That is something that we always would like RDFIs to be aware of and to use is that same day ACH returns. The faster we can get information back to the other party, the faster we can identify potential fraudulent situations, potential fraudsters, and get them off the network.

Keith Barnett: All right. Jordan, that was great. Thank you for this first episode. And thank you to all of our listeners for listening to us on this first episode. We want to make sure that you tune in to part two of this series where we will discuss fraud monitoring. And don't forget to visit our blog, troutmanpepperfinancialservices.com, and subscribe so you can get the latest updates.

Also, please be sure to subscribe to this podcast via Apple Podcasts, Google Play, Stitcher, or whatever platform you use. We look forward to part two.