ICANN Transcription

Transfer Policy Review PDP WG

Tuesday, 10 August 2021 at 16:00 UTC

Note: Although the transcription is largely accurate, in some cases it is incomplete or inaccurate due to inaudible passages or transcription errors. It is posted as an aid to understanding the proceedings at the meeting, but should not be treated as an authoritative record. Attendance and recordings of the call are posted on agenda wiki page: https://community.icann.org/x/ZQTpCQ

The recordings and transcriptions of the calls are posted on the GNSO Master Calendar page http://gnso.icann.org/en/group-activities/calendar

JULIE BISLAND: All right. Well, good morning, good afternoon, and good evening. Welcome to the Transfer Policy Review PDP Working Group call, taking place on Tuesday, the 10th of August, 2021 at 16:00 UTC. In the interest of time, there will be no roll call. Attendance will be taken by the Zoom Room. For today's call, we have apologies from Sarah Wyld, RrSG; Crystal Ondo, RrSG; and Mike Rodenbaugh, IPC. They have formally assigned Jody Kolker, RrSG; and Essie Musailov, RrSG as their alternates for this call and for the remaining days of absence. As a reminder, an alternate assignment must be formalized by way of a Google Assignment form. The link is available in all meeting invite e-mails.

All members and alternates will be promoted to panelist. Members and any alternates who are replacing members, when using the chat feature, please select either “panelists and attendees” or select “everyone,” in order for all participants to see your chat and for it to be captured in the recording. Observers will remain as an attendee and will have access to view chat only.

Alternates not replacing a member are not permitted to engage in the chat or use any of the other Zoom Room functionalities, such as raising hands or agreeing and disagreeing. If you are an alternate not replacing a member, please rename your line by adding three Zs before your name and add, in parentheses, “alternate” after your name, which will drop your name to the bottom of the participant list. To rename yourself in Zoom, hover over your name and click “rename.”

Statements of interest must be kept up-to-date. If anyone has any updates to share, please raise your hand or speak up now. If you need assistance updating your statements of interest, please e-mail the GNSO Secretariat. Please remember to state your name before speaking for the transcription. Recordings will be posted to the public wiki space shortly after the end of the call. And as a reminder, those who take part in the ICANN multistakeholder process are to comply with the Expected Standards of Behavior. Thank you and over to our chair, Roger Carney. Please begin.

ROGER CARNEY: Thanks, Julie. Welcome, everyone. Just a couple items I wanted to bring up before we get moving onto our agenda. Berry sent out the updated project plan last week. Just wanted to see if anyone had any questions or comments about that. Again, staff is doing a great job on keeping all of our work moving forward there. That should really help out, that project plan—show us where we're moving to. So let me know. Let us know if you have any questions or comments on that. Otherwise, we'll move on to …

I think last time it was mentioned that calendar invites for upcoming meetings … I think everyone should have received invites, I think through October now, at least. So if you haven't, please ping staff and they can get you hooked into those invites for that. I think that was about it. I think we can probably jump into our discussion.

Last week, we closed the comment period for early comments from all the stakeholder groups. And we did receive several comments. We just wanted to spend a few minutes here to address any of those comments—anybody that provided comments, anybody that works in our stakeholder groups that provided comments, if they want to speak to them.

We're focused on just the Auth-Info ones for now, since we are trying to wrap up that section. So if anybody wants to bring up any of the Auth-Info comments … I did read through most of them and I didn't see anything that we haven't touched on already or hasn't been mentioned previous. But if the authors or the authoring group wants to talk, I invite them to come up and speak to their comments, again focused on the Auth-Info comments. So if anyone wants to come forward … Jothan, please go ahead.

JOTHAN FRAKES: Yes. Thank you. You can always count on me to step up. One piece that I did want to comment on is that there is a new standard out. I'm looking for the specific standard raised by a security organization, suggesting … I think we had suggested in this about including dictionary words. And there was actually a recommendation by security experts about using three different dictionary words together in a string being just as secure as security strings that would contain random information. So I want to find that link and include that here, just for reference. But I did want to comment on that here, that maybe we don't include the dictionary word restriction. Thank you.

ROGER CARNEY: Okay. Great. Thanks, Jothan. Okay. And again, I think all the comments were really well-written, and again, I think just mostly supporting what the groups have already discussed. I didn't see anything major in there. But again, I invite anybody that wants to speak to and can come to the mic and speak to them. Otherwise, I think we can move on from the comments. I didn't see anything new out of them for Auth-Info. Okay. If no one has anything, we can move on and we can mark our Auth-Info discussion as complete for now. And we will revisit it as needed, as we go through the remaining items and as we wrap up, obviously.

All right. So let's jump into our major focus today on the losing FOA. Hopefully everyone read through this. Staff, again, provided a working Word doc for our discussions and comments as we make progress through this. So please feel free to comment, add any suggestions in here, as we continue our discussions. But I think we can just go ahead and jump in.

Can we scroll down to the charter questions? Do we have those in here? Okay. There we go. Okay. So let's just go ahead and jump in. And again, we'll try to do this similar to Auth-Info—now our TAC, Transfer Authorization Code discussions that we had. We'll briefly go through these and then we'll get into some good, detailed discussions as well.

Our first charter question, A7, is, "Is the losing FOA still required? If yes, are there any updates necessary?" And I think something to focus on, maybe, here—I've heard this in several discussions—is the losing FOA being required, versus being optional, versus not existing at all. So I think I'll throw that out for discussion with this topic. Is it still required? I guess we take the stance that current policy stands unless we have an agreement to change it. So current, the requirement is a losing FOA has to be sent for every transfer request process.

So I'll invite anybody to come to discuss their thoughts on keeping it or if they prefer to remove the requirement for the FOA. Again, is that a complete removal or is it an option move? So I'll open it up. Theo, please go ahead.

THEO GUERTS: Yeah. Thanks, Roger. I'm looking at this practically. We're already using the losing FOA for a couple years now since GDPR. It seems to be working all right. Of course, if you go for the optional, get rid of the FDA, then there's some extra work involved—could be to some, some consequences that nobody anticipated, though on the other hand, here in the Netherlands, for .NL, we don't use FOAs at all. It's just transfer the domain, enter the correct Auth

Code, and it's instantly—five waiting days, etc. So that seems to be working, in this region of the world, pretty well. But for now, practically speaking, let's don't change it.

It works pretty good. When I look at our numbers on how many people use the losing FOA, there's 85% of people actually responding to it and not just wait until it gets done automatically, the transfer. No. 85% actually respond within the five business days. So that's pretty high uptake of people using it. So yeah. I figure that's of use. Thanks.

ROGER CARNEY: Great, Theo. Thank you. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yes. I don't think it's required in today's world, with privacy and data loss changing across the world. But yeah. I agree that if it's not broken, let's not try and get more issues involved in terms of trying to get rid of it. I think it just makes more sense to just potentially leave it as it is or leave it down to the registrar to make that decision. Thank you.

ROGER CARNEY: Okay. Thanks, Keiron. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. The FOA is a security mechanism but it also delays the transfer up to five days. Personally, I think it would be nice if it would be optional because I like that we would be able to do it faster and more efficient than today. But I also don’t want to take it away from registrars that think the security feature is still necessary as their registrar Thank you.

ROGER CARNEY: Thanks, Kristian. I guess I skipped over—just an assumption, maybe a bad assumption on my part. I know a lot of people here are really deep into the transfers and know the process well. But I guess we should probably explain that the losing FOA … In the process, there’s a gaining FOA, which the gaining registrar, pre-GDPR, used to send, or even if they still can, send to the registrant to confirm their want to transfer.

And the losing FOA was maybe even a little looser than that. It’s weird that it’s not a form of authorization. It’s more of an acknowledgement that, “Yes. I agree that this should have been transferred.” It was more of a post-effect than a pre-effect. I don't know if anybody want to describe their process differently than that. But the current transfer policy identifies those two mechanisms—the gaining FOA, which we’ll discuss later, and this is the losing FOA.

And it sounds like at least those that have talked so far think optional is maybe the one change that we could make to this moving forward, as it is required today. But I’ll give people thoughts on that. Come to mic if you don’t like that it’s optional or if you’d prefer that it has to be required. Let’s get that discussed as well. Tom, please go ahead.

THOMAS KELLER: Thank you. I would prefer optional as well. The main reason is that there's already enough, I would say, time slack in the whole process. That's one of the main reasons why people are calling us up, that, "They gave us the Auth Code. Something's happening." And then, nothing's happening, really, for up to five days. So the registrars that even wait for the five days, if the registrant is saying, "Yes. That's all fine. Please move on …" It's very complicated for us to explain what's going on there. And if we have a mind that discussed making the transfer process a bit more near-time or real-time, I think this is not the right vehicle.

So if people want to use it, that's fine. But then that would be different with every registrar. So optional is not really an option, if you ask me, because each registrar will treat it as he seems fits and it will be very, very hard to explain that to any customer.

ROGER CARNEY: Great. Thanks, Tom. Okay. Jothan, please go ahead.

JOTHAN FRAKES: Yes. I think the thing to avoid here would be—if we did eliminate this or make it optional—would be the situation where you've got a registrant and the name was transferred away. They had no form of notice, or awareness, or control to stop that from happening if it was not a legitimate transfer. I think we want to be cognizant that we don't eliminate that there is some notice and that there is some means to decline as part of that process, in order to appropriately protect the registrant from having a name transferred away under non-normal circumstances. Thank you.

ROGER CARNEY: Great. Thanks, Jothan. Tom, I assume that's an old hand. Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. I'm not sure if we have that anywhere in our documents already but I just wanted to introduce a fourth option. Instead of taking away, optional, or keep it, we should maybe also think about if we could make it better, if we keep it. And one way to make it better, where we can also make transfers more efficient, is to require that it is as easy to accept the transfer as it is to deny it because then, if we have the losing FOA and it's easy for the registrant to click and accept the transfer, it would go through right away and it would then still be more efficient than today but we still keep the security of the losing FOA. Thank you.

ROGER CARNEY: Thanks, Kristian. Good idea. Jim, please go ahead.

JAMES GALVIN: Thanks, Roger. As I listen to some of the conversation, I'm thinking about your introduction to this topic, Roger, and your comment about the losing FOA serving as an acknowledgement that you really wanted the transfer to take place. I guess the question that I would ask here—because I think people have … In this discussion, I've heard a couple of different answers to this question. And that is what problem are we trying to solve? What is it we're trying to achieve? If you're going to keep the losing FOA, what reason are you keeping it for? Why is it there?

Among the reasons that I've heard here, "Well, it serves as nice evidence about the transfer." It's like, "Well, that's interesting." But there, you should keep log files. That ought to cover that, one would think.

Another possibility is it serves as a two-factor kind of thing in the transfer process. Well, that's interesting. I would question whether or not that's really a risk that has to be addressed. But that's a topic of conversation.

We've also heard references to, "Well we don't need it because the Auth Info covers it." And if we use the Auth Info properly, then you can meet the needs of getting authentication. You can also meet the needs of being able to deny it, if that's the case. You can meet the needs of … The way in which you present the Auth Info to the registrant can be that second confirmation process and whether they want to transfer to occur or not.

So the question that I'm asking is what are we looking to achieve here? It's not just about whether or not we want the losing FOA. It's what problem are we trying to solve? I'm thinking that there might be other ways to solve the problem, depending on what agreement we have about the purpose of the losing FOA. Thanks.

ROGER CARNEY: Thanks, Jim. And thanks for bringing up the discussion on the Auth Info, the TAC. Obviously, we've gone through that process and talked through it. I think that taken in light, those discussions where we ended up with … Does that help this discussion of the losing? Can we get onto a, "Yes. The losing is no longer all that needed?" Obviously, it is a security mechanism, as people have mentioned. Is that a needed security mechanism? Someone mentioned maybe it's optional one that someone wants. But with the TAC being more secure—or, I guess, more standard and secure—through our discussions, does that solve part of this losing FOA? Tom, please go ahead.

THOMAS KELLER: Thank you. I think these are very interesting questions—what we're trying to solve with that. At least my interpretation, so far, was always that this was meant to be a second factor so that if a transfer is initiated, that really the domain owners asked about that before it really happens.

So that begs the question when the right time is for that. You can either do it once the transfer has been initiated with the transfer code or before the transfer is initiated. So basically, you could also put it in front of the process and start with it instead of doing it at the very end of it. So even if we would stick to it, it's a question at what point of time we would like to send it out.

ROGER CARNEY: Great. Thanks, Tom. I think that goes along with what Jim was saying, as well. Is it actually being handled or could it be handled in another process? Kristian, please go ahead.

KRISTIAN ØRMEN: Thank you. When Jim was talking, I was just thinking if we have any numbers on how many transfers that are being rejected in that process today. I guess that probably the registries would be the best source of that information.

ROGER CARNEY: That's interesting. I don't know that we have any numbers on that, Kristian. I'll open it up to the floor and maybe staff, even, if they have any idea if there's any numbers. Theo mentioned that through his registrar, that they get about 85%. That doesn't mean either way, I assume, Theo. I assume that's just an 85% response rate, accepting or denying it. So I don't know if anyone has numbers like that. So, Theo, please go ahead.

THEO GUERTS: Yeah. The 85%, that is a confirmation to transfer away right away, within the five days. So they don't wait. They confirm actively by clicking on a link in the e-mail address, "I want to transfer right now. I'm not going to wait until it's done automatically." So that is 85% active participation.

ROGER CARNEY: Great. Thanks, Theo, for the clarification. Tom, your hand's up. Do you have another comment? No? Okay.

THOMAS KELLER: Sorry. I'm really bad with that.

ROGER CARNEY: That's okay. Thanks, Tom. Theo, your hand's up.

THEO GUERTS: Yeah. I was still going through the points that Jim Galvin made. I think when you dissect all those points, and if you go through this chart that we see here with yes and no, and if it is an extra layer of security or not, I think if you drill it down, there are many answers to a whole bunch of questions. And there will be registrars using it for the right and the wrong reasons to have a losing FOA or not. I think we boil down and circle back to the point like, "Let's make this optional." At least that way, the registrar has a choice to either use it or not.

If I think a little bit further along the way, if it would be optional for us as the Dutch registrar, I think I would lose the FOA so that I can bring it in line with the national ccTLD here, .NL, which is instantly … From a registrant perspective, a customer perspective, that would be much more in line for much of our resellers. So the entire process would be easier to explain for the majority of the Dutch registrants. Of course, every other ccTLD has a different version of the transfer process but the majority—the bulk—process-wise, would be very similar to what we have now, if done correctly. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Jody, please go ahead.

JODY KOLKER: Thanks, Roger. This question is pretty … I guess I want to answer it as it depends. If the losing FOA is completely taken away, or the option to be able to send that, then I would want to make sure that the registrars at least have five days when an Auth Code is requested to either not send the Auth Code at all, because it's fraudulent, or to send the Auth Code. It gives the registrars a chance to be able to determine if this is a fraudulent request or not. That's if the losing FOA has is just completely taken away. If that was to happen, I would still want to make sure that we have five days—the registrars have five days to send out the Auth Code, to be able to review the request.

Also, if it goes away … I think Jothan might have alluded to this. But if that is to go away, I would want some way to be able to get that domain name back if the registrant is only notified that the domain has been transferred after it's been transferred. Somehow, we would need some kind of way—the registrars—to be able to claw back that domain name for a registrant that has had that taken away.

Whether that's a board, or connection with the registry to be able to say, "Hey. We need that domain name transferred back," but it has to be something to be able to allow that registrant to get the domain name back, whether it's through review by a group of people, or whether it's the DNS replaced to what it previously was until a review is done. I just think there needs to be a lot more discussion on what it means if we completely take the FOA away. Thanks.

ROGER CARNEY: Thanks, Jody. And thanks for teeing that up, actually. If staff can scroll down to the additional questions section, there are a few other prompting questions that Jody hit on, actually. I don't know if he intentionally did or he just accidentally got into those—but some other questions for consideration. I think we can go through those as well. Just take a look at them. And as Jody mentioned, the first one, does that five days still exist and things like that. So just take a look at those and we'll cover them as well. Theo, please go ahead.

THEO GUERTS: Yeah. Thanks. What Jody just mentioned, I think we've been trying to solve that issue for more than a decade, actually. We've never really gotten very far on that subject. Of course, points that Jody mentioned are still valid. But I think that the losing FOA and the five days, when is it ever going to be enough?

If you're dealing with some criminal actor who knows what they are doing, and they're covering their tracks really well, usually what you see in those high-profile cases, they discover that the losing party—the losing registrant—goes six months later, "What the hell? My domain name has been stolen a long time ago." Then is when usually they discover that the DNS has changed and they have lost control over the domain name a long time ago.

So making sure that that domain name doesn't get transferred illegally or be stolen, that's very tricky to protect the registrant from that. But I think that Jody is correct and maybe we can get some headway on this in this PDP. How do you invent a process that if all things went wrong and all security measures were bypassed, how do you get it back? I think that's a valid point and I think we should discuss that. Thanks.

ROGER CARNEY: Thanks, Theo. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yeah. I think five days, in the current standard, I think is probably right. From our registrar, I've seen people essentially come even two to three years later, stating the fact that their domain was transferred, as I'm sure many other registrars out there have as well. How do we put limits on that as long as people have renewed? Again, if the domain is that important to you, how long do you go without realizing that it's no longer in your possession? So yeah. I think there's lots of questions to answer there, just in how we want to tackle that.

But again, I've also reached out to registrars in terms of where domains have potentially been stolen. And not to name anyone, but most seem very complaint and understand the aspects of what's happening. And these escalations do normally go to, or if the person does choose to, it can go to ICANN and stuff like that.

So I think there's lots of areas where we could potentially look into here. But yeah. I think it's just in this section, how far deep do we go into it. You could probably do a whole other PDP on this in itself. So yeah. I just think we should probably delve into but not do a deep dive, if that makes sense.

ROGER CARNEY: Thanks, Keiron. Okay. Any other comments, as I read through these additional questions, I see we've hit on several of them. The five-day, I think that we even talked about the five-day when we discussed the TAC as well. And people thought … Yes. Some more discussion. Holida, please go ahead.

HOLIDA YANIK: Yeah. Thank you. I want to add that in terms of contractual compliance, the elimination of losing FOA would highly impact investigations, especially of unauthorized transfer complaints. Since GDPR, we are having different processes when addressing the cases with gaining registrar after the gaining FOA is not being processed currently. The main burden is laid now on the losing registrar and provision of this losing FOA. So I want to add this item to the discussion, also.

ROGER CARNEY: Great. Thanks for that, Holida. That's good information. Steinar, please go ahead.

STEINAR GRØTTERØD: Hi. I find it very interesting what Theo said because if I understand him correctly, it's that the five days will not actually solve any crime when a domain name is highjacked because, most likely, the registrant—the correct owner—will not identify this within the five days. So I'm just curious whether we can solve the crime issue with this new policy in this section. Maybe that's more into the transfer dispute process. Thank you.

ROGER CARNEY: Great. Thanks, Steinar. And as Steinar just brought up, we do have, in our later phase, a discussion around the dispute mechanism, which I think even some of what Jody brought up will be discussed more in detail—how that process is, what happens during that process. As he mentioned, do you just change the DNS back? What are those options. I think that we'll get into a good amount of detail once we hit that dispute mechanism idea. Jim, please go ahead.

JAMES GALVIN: Thanks, Roger. Some more questions to ask about this transfer process and even related to this losing FOA. The question is what problem are we trying to solve? I want to ask what has failed when it's necessary for a transfer to be recalled? And I ask that question for the following reason. Is it that the transfer itself was somehow bad, meaning did the transfer process work as it was supposed to and yet there's some other external pressure that wants it to be recalled?

So did the user lose control of their e-mail? Did the registrant lose control of their e-mail, and as a result of all of that, somebody was able to negotiate getting things around? Did the registrant break into the registrar? Did they hack into the registrar's account? If you're going to hack into the registrar's account, at that point, it seems to me all bets are off. Does the transfer process itself have to accommodate that? Is that the motivation for this five-day window, that I have to make sure that it's a valid transfer because I have to check all of these externalities?

It seems to me if there are externalities that have come to bear, I appreciate that that's a customer service problem. Don't get me wrong. I just want to call out this issue. I want to call out this question. What is it that is the motivation for wanting to claw it back? What is the failure that has resulted in the need to claw back the domain?

To me, that factors into how easy or hard the transfer itself needs to be and the recovery needs to be. Maybe the recovery process is you've got to go to ICANN and complain and they can deal with it because it's not the transfer process that was broken. There was some other externality and the transfer process doesn't have to fix the externality. So that's my question to examine here. What's motivating the need to claw them back? Thanks.

ROGER CARNEY: Great. Thanks, Jim. And I'll open that up for registrars. I'm sure most of the registrars have experience into the reasons why. But to your point, Jim, I don't think there's a failure in the transfer process itself. It is an external, as you called it, factor that has caused that. Again, I don't think there's a systematic or even the policy itself is broken. It's just that someone has found an external—as you describe it—external way to affect that. Greg, please go ahead.

GREGORY DIBIASE: Yeah. I think Jim makes a good point and I agree. In my experience at least, when a domain has been improperly transferred, it's usually and account compromise. The e-mail is compromised as well. So the transfer process works. It's not because there was some issue with the transfer process, like the registrar sent something to the wrong e-mail. It was a compromise. So I agree with Jim. I don't know if Jim was saying this but I'll go further and say that because of this, I don't think we're necessarily going to find a solution to that problem in the transfer policy, if that makes sense.

ROGER CARNEY: Thanks, Greg. I think that does make sense. I think that what, to this group … And we don't have to decide it now. It's one of those where I think, again, we'll discuss it in the transfer dispute mechanism. But I think as Jim even mentioned, maybe the recourse is, "Take your complaint to ICANN." But I want to see if this group comes up with that process of … Okay. We know that happens. Those external factors do happen. Does this group see the need to create a process that people can follow when that does happen, since we do know that it happens? Theo, please go ahead.

THEO GUERTS: Yeah. Basically, when you look at a process, regardless of what process we invent here, we could come up with a transfer process that would be very secure. But the reality is, that will be bypassed at some point. There is not process that is so secure that it can never be bypassed. Criminals will always be in a position to steal in a domain name, if they really want to, for whatever reason.

So basically, you come back to the question that Jody already mentioned. If it has happened, how do you reverse the situation as soon as possible. That's when usually the hurt starts. Suddenly, phishing pops up on a domain name or whatever malicious activity or dramatic activity was going on, which is not in the best interest of the registrant. The company page is suddenly completely wiped out or whatever. We can come up with a dozen—couple of very dramatic scenarios here. But basically, the question is if it happens—and it will always happen, regardless of what we invent—how do you undo the damage? That's be an ongoing discussion for longer than ICANN. I haven't heard a solution yet. Thanks.

ROGER CARNEY: Great, Theo. Thanks a lot. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Yes. I think a lot of the way that we're going here as well is that a lot of the onus, as well, has to be on the registrant. I've dealt with people in the past who have explained that they've given their password to family members to transfer things away. I know people who have just literally given passwords away. And I have e-mail correspondence with them stating that. So there was nothing wrong with the actual transfer process or anything like that. It's how far are these individuals prepared for their own security as an individual. I think we also have to take that into consideration as well.

Putting more security steps in place may work. But again, if people are prepared to give passwords—if registrants are going to give their passwords away—how far to do we go before we say, "Okay. Enough is enough. If you believe that this has been stolen, then you may need to go to your local jurisdiction, file a complaint, or take it to court," because of however that is processed. I've got numerous cases that I can think of over my years of doing this where how do we actually protect …? We can't protect everyone. It's impossible.

So moving forward, maybe the transfer process isn't the right issue to be explaining this. Maybe we could add an additional security measure in, like I mentioned. But again, a lot of this, as well, has to be down to the registrant.

ROGER CARNEY: Great. Thanks, Keiron. Tom, please go ahead.

THOMAS KELLER: Thank you. Yeah. I think there's two separate questions, basically. The one thing is if the transfer is really fraudulent, malicious, or however you want to call it, how can it be reversed? And I think that's on our topics of to-dos as well, as we dive into. So once the complaints have come in, people claim that the transfer was fraudulent. That could go in both directions—so people claiming that it was fraudulent even sold the domain name, for example. We've seen cases like that before. So I think we have to be very careful how we can construct something that is reversing transfers.

But going back to the original question, at least from what I've heard from a lot of people, is that they deem it as a second factor. So if it is a second factor, I think we should ask ourselves whether this is the right second factor or what second factor we would like to have in the future. Just because it's always been there, it's not the best reason, actually, to keep it.

At least from my recollection, I think the five-days' window was there before the transfer policy and the policy we have in place currently was even introduced. So it really comes from back in the day and it has never been questioned. The question is, for us, whether we just want to keep on having it because we always had or whether there aren't smarter ways if you view it as a second factor. Thank you.

ROGER CARNEY: Great. Thanks, Tom. Theo, please go ahead.

THEO GUERTS: Yeah. Thanks. I'm maybe not suggesting to reverse a process, what we are doing here. But at some point, if we are going to look at the transfer dispute policy, I think it would be helpful because then we are actually looking at it. From what I remember, back in the day, when we were working on it, it was shortly after IRTP-C and we didn't spend a whole lot of time on the transfer dispute thing, if I'm completely honest.

It looked good on paper and everybody agreed on the IRT. But I got this gut feeling, if we go back to it now and we look at it, there's probably a lot of stuff that, with the collective minds here together, we could actually improve that thing a lot. And maybe, therein lies the solution for a lot of the questions we are trying to get answered on this call. Thanks.

ROGER CARNEY: Great. Thanks, Theo. We'll definitely visit that later in the PDP. So it is something to keep in mind and keep those thoughts moving. And obviously, it sounds like it's a necessary thing, from what people are saying—as Theo mentioned, maybe not the exact one we have today but it is a necessary function that we're going to need. And as Jim brought up, maybe that doesn't mean the transfer process gets more security mechanisms but just a more streamlined dispute process.

One of the other things I was curious about—hitting back to Jim's purpose, I guess—is the frequency that this happens is how often? Out of the thousands of transfers that occur, how often is there an actual claw-back required, to the point of does that mean additional security measures are needed because it happens so often? Or it's infrequent enough that a good dispute policy would resolve that? Jim, please go ahead.

JAMES GALVIN: Thanks, Roger. It occurs to me to try and frame my comment about externalities a little bit differently. Maybe this will be helpful to the overall big-picture architectural question. I think that security and the need for security is really a holistic kind of issue and a holistic kind of problem. Part of the reason why I bring up the question of externalities is because we should focus on the transfer process and making it be as effective as possible. But whether or not you have other external issues is about a holistic security view. We want transfers to be secure but that doesn't mean that transfers have to solve every problem that might result in a bad transfer, or a transfer that was undesirable, or a transfer that was unneeded.

I do think that if a registrant's account at the registrar is compromised, then frankly, all bets are off. Nothing we're going to do here is going to fix that. Even the losing FOA doesn't fix that in a strict sense because if you've lost the account, then I can change all the e-mail account addresses, all the addresses that are going on there. Unless you're applying other kinds of security controls, you don't allow those kinds of changes without confirming them in some out-of-band, second-factor way.

And I would presume, quite frankly, that not everyone has all of these extra levels of process built in. You probably don't really need them, on average. I don't think that everybody has to have the most secure services and the most secure holistic service. Not everybody wants them. Not all domains are that important. It's a risk management problem.

But that's why I focus on what's the purpose of a losing FOA and what are the externalities that cause the transfer to be bad? Because they're probably not problems that you can solve with the transfer process. The transfer process is going to work and it's going to work smoothly. It can work in a high-volume way, in a secure way. And bad things are going to happen because there's other bad vulnerabilities and other opportunities. We can't deal with them in this process. That's what I'm focused on.

By the way, the SSAC response that was sent into this group, it actually referenced a number of documents that actually do speak to various things related to Auth-Info codes. And it also generally speaks about registrant protection. There are a number of documents that were included in there, that have some of this discussion about these kinds of externalities that come to bear on a registrant. And that's why it occurred to me to suddenly say something about this.

Try to reframe my externality discussion. We don't have to solve everything here and there are other discussions elsewhere that address this. I'm not even sure it's in scope for here. I don't know if that helps but just trying to put some words out there. Thanks.

ROGER CARNEY: Yeah, Jim. Just one follow-up for you. You've said "registrar account" a couple of times when you're describing that. I just want to clarify. Are you speaking of the registrar EPP account with the registry, or even the web portal registrar account, or are you speaking of a registrant's account at the registrar?

JAMES GALVIN: Yeah. Thank you for the question and the clarification. The latter. I'm talking about the registrant's account at the registrar. Thanks.

ROGER CARNEY: Okay. Great. And something Jim mentioned. If you do go through and read those comments, the SSAC does refer—and I'm just going to throw out a number—probably half a dozen different papers as it relates. Don't be deceived by the SSAC's comments as being short. They did put in a lot of references to prior discussions on all these points. So when you take a look at the SSAC comments, you will drill in quite a bit to what Jim mentions as a lot of those external things. So, Steve, please go ahead.

STEVE CROCKER: Thank you. I just want to add to the good comments that Jim has made and that you've also explicated there. The registrar account that we're talking about is actually a third-party person that is the account holder with the registrar. That may or may not be the same person as the registrant.

In the creation of a domain name registration, the account holder is the one who's doing the action, presumably on behalf of the registrant, if it's not the registrant himself. And then, there's a very interesting moment, which I think everybody on this call actually understands—a birth process in which the legal control passes from the account holder to the registrant, although the account holder continues to hold the keys to the account and could make changes.

So what this means in this context is two things. If there is an authorization to allow the registration to transfer, it might be coming from the account holder, it might be coming from the registrant, or it might be coming even from the admin contact. What's essential is that the registrant—the personal who legally controls this—has to be notified. This suggests that there's a step further back, which is if there's hacking going on in which there's a change to the contact information for the registrant, the registrant has to be notified quickly and reliably. That's a precursor to making sure that the registrant is then able to react if he's later notified that there's a transfer underway.

So what I'm saying is two things. One is with respect to the actual transfer, it's important to notify the registrant, even if the registrant wasn't involved in the action. Second of all, prior to that, there has to be a high degree of protection of the registrant contact information so that the registrant can be notified in the even that there's a transfer. Thank you.

ROGER CARNEY: Great. Thanks, Steve. And thanks for bringing up the nuance of the account holder and registrant as being possibly separate. Theo, please go ahead.

THEO GUERTS: Yeah. I mostly agree with Jim. No disagreement from me there. Just to add on, if you look at the account holder or the registrant account, if the OpSec of the registrant is bad, bad things will happen. And we can come up with a lot of policies with a lot of warning systems, like e-mailing the registrant that a transfer has happened. If the OpSec of the registrant is bad or not sufficient, then an attacker will make sure that the registrant will never see any notification, whatever it is—be it SMS, be it e-mail, or whatever. There are so many ways to make sure that a registrant does not get any alerts.

So if you try to bake this into all these processes right here, I think we'll go way off the path here and it will be not sufficient, ever. We will never reach the goal through a policy. We cannot come up with a policy that will make it so secure for the registrant that they will always be in a happy place. Like I said, if their OpSec is bad—and it can be for a million reasons. It can also be that the registrar doesn't provide sufficient protection, which would be a violation of several data protection laws and cybersecurity laws that are present or will be introduced at some point in other parts of the world where it is not present. So I think that is a moving target. That is not up to us. But from there, we cannot just come up with a policy that will be 100% ever secure. Thanks.

ROGER CARNEY: Great. Thanks, Theo. Okay. Any other comments, suggestions, discussion on this Again, as I look through these additional questions, it appears that we have hit on most of these. And it sounds like the losing FOA possibly being an optional concept for the registrars, I think we have to work on is that even something that needs to be put into policy or not.

It'll probably come down to people's opinions on does that help compliance and does that help the registrant and registrar during those compliance issues? If it is an optional piece, will a registrant complain that it's being too slow, that they're having to go through too many hoops? If we leave it completely out, and they make the complaint, and the registrar is just trying to use a losing FOA as an option, then they may get pulled into that complaint, whereas if it was in policy as optional, then there's something to lean on. So just thoughts to that process.

Again, it seems like people are leaning toward making the losing FOA optional and that, obviously, people are still looking for the five-day window—maybe not so much for the losing FOA but as the process of assigning or creating the TAC and providing that to the registrant, all as one concept.

Current text of the losing FOA. I think if were making it optional, the text becomes … Maybe we provide guidance but not necessarily specific text---again, if it's going to be option. And I think this was talked about as well.

Should the losing FOA require express authorization confirmation? And I think this question goes back to what Theo's saying. A lot of times, 85% of his customers are clicking, "Yes. Let's transfer this," and then it goes instead of waiting for five days. And I think that that's what we heard is a good concept.

The paper trail? Again, I think we've talked about this in our discussions of the Auth-Info and TAC—this virtual trail, not a physical paper trail. And I think Jim mentioned it today as well, that logging should, obviously, account for this. Are there any requirements that we would make, in addition to the current ones, for transfer—for logging, to create that virtual paper trail? Just something to think about is do we need to add any specific language that states, "You must keep the audit trail around—the logging around?" And again, is there any change to the current wording in the policy?

Any other security mechanism? We talked about how this FOA gets integrated in. Again, any additional comments, questions on this? Zak, please go ahead.

ZAK MUSCOVITCH: Thank you so much. Just in terms of gauging people's reaction to whether to make the FOA optional and whether to keep the five-day, my read of the conversation so far is a little different. It seems to me that there's an opportunity, really, to simplify the procedure, get rid of the FOA, perhaps entirely, and put the emphasis on how other people mentioned the superior dispute resolution policy that deal specifically with theft.

So, for example, from my perspective, if there was something like a UDRP for domain name theft, that would enable me to put far less emphasis on the meager security that's offered through the transfer policy. As other people pointed out, if that gets penetrated, [that's rough]. Thanks.

ROGER CARNEY: Great. Thanks, Zak. That's greatly appreciated. I think that you're right. I think that's where this is heading. Is it optional or is it just going away? I think that's a good point. Theo, please go ahead.

THEO GUERTS: To Zak's point, I think we already have that. It was part of IRTP-D, where the dispute provider would actually look at the case and then come up with a verdict within x amount of time. There was some money involved, also. It looked very much like the UDRP process. A lot of UDRP people were involved in that through either the IPC, or IP lawyers, etc.

I think that is worth looking back at again. Like I said, that process was a little bit rushed and maybe we can improve that a lot. It's far from perfect now. I think it's never been used or one time. So in all these years, that process has never been really triggered, for whatever reason. So yeah. I think we should circle back on it and see if we can improve that process.

And regarding the FOA as a paper trail, when there is account takeover or e-mail takeover and a hacker clicks "yes" to transfer, what is the worth of an FOA as a paper trail then? The hacker acknowledged to the transfer on date x, time x? That's not very useful to me, I think.

ROGER CARNEY: Thanks, Theo. That makes sense as well. Zak, is that a new hand?

ZAK MUSCOVITCH: Lowering it. Thanks.

ROGER CARNEY: Thanks. Berry, please go ahead.

BERRY COBB: Thank you, Roger. Just a couple of observations here and try to work backwards. First and foremost, the TDRP, the Transfer Dispute Resolution Process, Theo is right. I think it even somewhat existed before IRTP-D but it wasn't used hardly at all. There were revisions to it. And even to date, I believe we can find or pull the stats from the policy status report that it has still not been used very much. I can't speculate as to why it hasn't been used much.

But in general, the procedure itself is between the gaining and losing registrars. It's only initiated, I believe, by the losing registrar, where the registrant, or their customer, has exhausted all other possible options to try to recover the domain.

So certainly, as Emily pointed out, that's something that this group will take a look at in closer detail in phase two. There's nothing to prevent the group here, at least cursory talking about it in phase one and giving ourselves an internal recommendation for us to consider or pointers, when we do discuss it in more detail in phase two. So I'll leave that there, for the TDRP.

Finally, in terms of changing the existing requirement on the FOAs … And I know we're nowhere near to trying to determine preliminary levels of agreement, or consensus, or anything like that. But I just do want to remind the group here that the losing FOA and even the gaining FOA are existing requirements. Of course, the gaining one, there is a moratorium on compliance enforcement for the gaining FOA. But the losing FOA is a still requirement. And just to remind here that it will take at least consensus, if not almost near full consensus, to change that existing requirement of the losing FOA—to convert it from required to optional or to sunset it altogether.

And then, finally, I think what is being referred to as the paper trail is a very important factor. And I would encourage this group—especially the registrars—to provide examples of logging on transfer transactions that could replace, or replicate, or that could be useful in terms of investigating improper transfers so that we have a better understanding of what we're losing and what we're gaining in terms of a logging and a breadcrumb trail to what happened. I hope that was useful. Thank you.

ROGER CARNEY: Great. Thanks, Berry. Just to add onto that, obviously, we can discuss—we're going to discuss in detail later—but all these items that come up, anything we discuss, we'll pull forward into those discussions. So if we have good ideas here on the dispute mechanism, we can pull those forward when we actually get into that detail.

One thing that someone mentioned earlier was today, it's the losing registrant's responsibility to prove everything here. So if they think something went wrong, it's up to the losing registrar. So something to think about here is, is that responsibility in the correct spot? Should the gaining registrant have some ownership in any dispute as well? Just, again, something we'll cover in the dispute but something to think about. Okay?

Great. That was a really great discussion. And again, probably the biggest question here for us—charter question on this section, anyway. And as Berry mentioned, we're not making any decisions here. We're just discussing what hopefully leads to easy conclusions. But we'll make those later. This is just for discussion.

All right. Let's go ahead and move on. We've got about 24 minutes to go. Let's jump into the next charter question and see if we can get a discussion going. Charter question A8 is, “Does the CPH-proposed TechOps process represent a logical starting point for the future working group or policy body to start with? If so does, it provide sufficient security for registered name holders? If not, what updates can be considered?”

One of the things on this charter question here is we’ve already hit on a lot of these things when we talked about the Auth-Info specifically. We saw some benefit or some good acknowledgement that the paper did provide some good direction for the TAC, at least. And I guess we need to look at here as well. Does it provide any good, useful direction for the losing FOA as well? As noted here, highlighted, the TechOps group agreed that the requirement to notify the registrant about a transfer request should be mandatory.

I don’t think it got into … And maybe Tom can help here. I don’t think it got into the specifics about that notification—how that should happen. And something to keep in mind is what Steve brought up as well. The account holder is different than the registrant. And here, we’re specifically speaking about the registrant being notified. And again, as Jim brought up, what are we trying to solve? Where are we going to solve this at? Does the notification have to be done in a losing FOA or can it be done in the process along the way?

Again, I’ll open it up for any discussion on this. I think that, obviously, a registrant notification is great. Where that happens and how it happens, I think, is the bigger discussion. Any comments, questions on this discussion? Jim, please go ahead.

JAMES GALVIN: So I'll ask a question similar to what I was asking before about all of this, which is what are we trying to solve by saying that they have to be notified? Given also the distinction that Steve was making about registrant versus registrar account holder, if you're going to notify them, all of that is interesting. But what are you trying to achieve by notifying them?

Arguably, the Auth-Info code and the fact that you have it in your hand represents the fact that you've been notified because you got the Auth-Info code, assuming you've set up processed for the registrant to get it. So therefore, I've been notified because now I've got it and I can now go and transfer this domain. Or am I trying to solve some other kind of problem? So that would be the question. What is the value of that notification? What is that adding to the process that's probably already there? Thanks.

ROGER CARNEY: Great. Thanks, Jim. Jothan, please go ahead.

JOTHAN FRAKES: Thank you. So I'll put on my co-chair of the TechOps group and say I think we wanted this there because it does represent something different, in that there is some notification happening. It is possible to obtain the Auth-Code in ways other than the e-mail request. And the notice would be something that would allow someone to be aware of the change.

Given all the changes—and I don't think it was entirely evident to us just how that would manifest, in light of how GDPR cascaded across our industry—the objective here was, as I mentioned earlier in the call, to ensure that a domain just doesn't silently vanish and that it serves as some sort of a documentation that this is happening. So some sort of notice would help in this case. I think it is different, materially, than … You can't just assume that because somebody has the Auth-Code that this is a compromised e-mail.

ROGER CARNEY: Great. Thank you.

JOTHAN FRAKES: Thank you.

ROGER CARNEY: Maybe I missed this part on reading it out. But one of the other items of this was that it didn't necessarily have to be sent in an e-mail. TechOps is suggesting that possibly other options of communication may be more useful or may be more relevant moving forward in time. So something else to think about. Theo, please go ahead.

THEO GUERTS: Yeah. What Jim just said, what are we trying to solve? If the current process would be as broken as hell, I would say, "Yeah. This is pretty much required and could be a solution to talk about."

But I don't see what this is going to solve. Also, unless it's going to be very specific … The process works, people. So I don't see any big issues there.

And notification, to put it in a different perspective, like I said, with .NL, the transfers are instant. There is a notification. In general, most people don't read it. It generates almost no support logs, like, "Why has my domain name been transferred?" We don't get any of that. So it's pretty much people are either okay with it, so either the process is working correctly and everybody's happy. It doesn't happen often that people react to a notification. So then, what is the use of the notification? It doesn't seem to solve much. Thanks.

ROGER CARNEY: Thanks, Theo. Jim, please go ahead.

JAMES GALVIN: Thanks, Roger. I just want to connect a couple of dots here. Part of what stood out for me, building on what Theo was just saying, is the question up there says that, "If so, does it provide sufficient security for the registered name holder?" I guess part of what I'm reacting to when I say, "What is the purpose of the notification?" is, in fact, explicitly in response to that question. I don't believe there's any security enhancement, per se, in notifying the registrant.

However, I don't want to suggest that I'm opposed to notifying the registrant. Always a follow-up. And the way that Theo described it, in fact, is ideal in my mind. When the transfer occurs, then you should send a notification and you should just say that it's happening. There's nothing wrong with that additional level of giving them a chance. Maybe that's part of your recovery process, is they have that opportunity for recovery.

However, from a risk management point of view, I'll now come back to the security question and ask again, still, what are we really getting here? Because the gaining registrar can't send that notification. It has to be the losing registrar that sends it. And if the losing registrar—or, I'm sorry, the incumbent registrar—is being badly-behaved, then none of this matters anyway. So you're not really gaining anything with this notification because they might not be sending it.

Again, if the problem was a registrar account compromise, all the e-mail addresses are changed anyway. Who knows what they're really sending the notification to and what's really going on? And the gaining registrar can't send it because, as Jothan said in the chat, they don't have access to the information that's already in the record. You don't have that information so you can't send it anyway.

So that's why it's this notion of security that causes me to want to lean on the question, what are we trying to solve? Not that notifications are bad but what is the benefit? From a security point of view, what is the benefit to the overall execution of a transfer process? If it's just an information notification, sure. What's wrong with notifications? They're a good thing. But if you're trying to derive something out of it, that's when I'm pressing on that question. What is that? Thanks.

ROGER CARNEY: Great. Thanks, Jim. Jothan, please go ahead.

JOTHAN FRAKES: Thank you. It's a new hand, new topic. It builds upon the bus that drove through the wall for us, which was GDPR and how it affects contact information. In the case of a thin registry, there is no awareness at the gaining registrar, necessarily, that some registrant is on both sides of this. So notice and notification can sometimes be affected by thick or thin registry as a factor.

So sometimes, in the case of thin registries, you have a change of registrant happening real-time, at the same time as a domain transfer. I think that that is a little bit different. And we need to identify that that does need addressing in the case of thin registries. Thank you.

ROGER CARNEY: Thanks, Jothan. Steve, please go ahead. If you're talking, Steve, we can't hear you.

STEVE CROCKER: Oh.

ROGER CARNEY: There you go. I can hear you.

STEVE CROCKER: I meant to lower my hand, not raise it. I'm sorry.

ROGER CARNEY: All right. Thanks, Steve. Theo, please go ahead.

THEO GUERTS: Yeah. Thanks. Of course, what Jothan brings up is a pretty interesting point and previously, pre-GDPR, we would be able to see what actually went down, if the domain name was not protected by privacy, anyways. But I wonder how valid that scenario is. We don't have any statistics about it. So basically, we go back to the point, what are we trying to solve here? I think it brings little to the table from that point of view. So yeah, again, what are we trying to solve?

ROGER CARNEY: Great. Thanks, Theo. Keiron, please go ahead.

KEIRON TOBIN: Thank you. Correct me if I'm mistaken but I believe that in terms of gTLDs, by the time this PDP finishes, they will all be essentially, thick registries. Like I said, correct me if I'm wrong on that but this is going to be around two years. So technical aspects, yeah. You never know. But I know it's in the pipeline for those. So yeah. I don't know how far we want to delve into something that essentially may not … By the end of when this finishes, it might not even exist.

ROGER CARNEY: Okay. Thanks, Keiron. Theo, please go ahead.

THEO GUERTS: Yeah. I understand the point that Keiron makes. It’s a good point. If it actually happens is a completely different question. But I think we should be agnostic enough in our policy work that that wouldn’t be a factor. Thanks.

ROGER CARNEY: Thanks, Theo. Yeah. And I think that that’s the hope. Obviously, we can think about that and make sure whatever we come up with fits that. And hopefully, we’re not being prescriptive into how the registry actually functions. All right. Any other comments, questions on this one?

Okay. We have about 10 minutes. Let’s go ahead and jump into the last one. It’s A9. “Are there any additional inter-registrar transfer process proposals that should be considered in lieu of or in addition to the TechOps proposal? For example, should affirmative consent to a losing FOA be considered as a measure of additional protection?”

Just to comment to the early input, BC mentions transfer lock should be removable by the registrant, in context of this question. So again, thinking outside … I think we’ve hit on a few items but thinking outside of what TechOps proposed or what we’ve discussed so far, are there any additional ideas around … I don’t want to say “security” necessarily. But any additional proposals to make this better? Theo, please go ahead.

THEO GUERTS: Yeah. I think we already have a lot on our plate already. So I don't think, necessarily, we need to take on more. If you talk about security—I mentioned that last week also—that is basically up to registrars or Contracted Parties themselves. They will be benchmarked against the law or whatever. And basically, when you talk security, Jim, or when you mention it, you need a holistic view there. So everything needs to match there. You can't account for everything. You can't account for what a registrant does on the Internet and how well-secured the e-mail address or their e-mail account is. Maybe they use the sloppiest password ever. We cannot prevent such things.

But all the other stuff that is on our plate, from a technical and legal perspective, yeah. I think the current landscape is now that we need to make sure that we are complying with everything we need to company with. And in most cases, we need to go above and beyond when it comes to security. Thanks.

ROGER CARNEY: Thanks, Theo. Keiron, please go ahead.

KEIRON TOBIN: Yeah. Just going back to the thick and thin registries, I'm just wondering whether it's worth reaching out to those registries that are thin, just to see their potential alliance, to see if they can give us any guidance in what they tend to do. Then that way, we may be able to potentially jump over that. I understand that they may not be able to give the answers that we're looking for. But surely, it's got to be worth a punt at this point, just maybe from the chair or something just reaching out.

ROGER CARNEY: Great. Thanks, Keiron. Okay. Any discussion? Does anyone from BC want to talk about the comment that was made from the early comment period around transfer locks? Zak? No.

ZAK MUSCOVITCH: Sure. What kind of comment were you looking for?

ROGER CARNEY: I just noted that the BC made a comment that the transfer locks would be removable by the registrant. I didn't know if there was any other details you wanted to provide into that comment.

ZAK MUSCOVITCH: I think that comment, just as it appears there, is kind of out of context. If you look at the balance of the comments, we get into it with a little bit more specificity. Really, the tenor of the comment is just that the opportunity to opt out should be more clearly telegraphed to registrants. There should be some uniformity and transparency amongst the practices so that registrars, registrants, and ICANN alike all understand.

That comment in particular isn't meant to say that there should be no transfer locks or they should all be removable in all circumstances. It's really within the context of some broader, more general comments. Thanks.

ROGER CARNEY: Okay. Great. Thanks, Zak. Okay. Well, I think that really was a good day of discussion. We made it through the three charter questions related to the losing FOA. So again, I think that … Steinar, please go ahead.

STEINAR GRØTTERØD: This is a short question about the comment from the BC. It is the registrant that always will have to remove any transfer lock. I assume you don't propose that the registry should remove a transfer lock when the transfer is initiated, automatically. That's not what you're asking about.

ZAK MUSCOVITCH: No. Not at all.

STEINAR GRØTTERØD: Perfect. Thank you. I was kind of surprised there.

ZAK MUSCOVITCH: Yeah. No, no. I think that these comments were pulled out from the broader comments so they could be easily misunderstood. But we're on the same page. Thank you.

STEINAR GRØTTERØD: Perfect. Thank you.

ROGER CARNEY: Great. Thanks, Steinar. Thanks, Zak. Theo, please go ahead.

THEO GUERTS: Yeah. Just a quick question that just occurred to me now. Do we need to specify what a transfer lock is when we are talking about a transfer lock? Is that a registrar transfer lock? Is that a registry transfer lock? Because those things are very different.

ROGER CARNEY: Thanks, Theo. Yeah. And I think we need to be specific. We've talked about both of those and we'll talk about them more as we go along. But yeah. I think that what we have to be specific about, when we do talk about those, is which transfer locks are we mentioning. And actually, when someone brings up a lock, what lock are we talking about? Maybe it's not a transfer. Maybe it's something else. And those things, we need to be specific about when we're talking about them. So thanks, Theo.

Okay. Again, great discussion. I think that getting through these at initial discussion is great. It'll give everybody some time to think about what everybody else has brought up as we continue the discussion next week as well. So I think that today was a great discussion. We'll let everybody think about it and we'll pick up here next week as well. So if there's no other comments or questions, I will turn this back over to staff and let us close us out.

JULIE BISLAND: Great. Thank you so much, everyone. This meeting is adjourned. I hope you have a good rest of your day. You can all disconnect your lines. Thank you.

[END OF TRANSCRIPT]