

**Registration Abuse Policies Working Group
TRANSCRIPTION
Monday 17 August at 14:00 UTC**

Note: The following is the output of transcribing from an audio recording of the Registration Abuse Policies Working Group meeting on Monday 17 August 2009, at 14:00 UTC. 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. The audio is also available at:**

<http://audio.icann.org/gnso/gnso-rap-20090817.mp3>

On page:

<http://gnso.icann.org/calendar/#august>

All recordings and transcriptions are posted on the GNSO calendar page:

<http://gnso.icann.org/calendar/#august>

Present for the teleconference:

Greg Aaron - Registry C. - Working Group Chair

James Bladel - Godaddy Registrar C.

George Kirikos - CBUC

Mike O'Connor - CBUC

Roland Perry - Individual

Berry Cobb - CBUC

Faisal Shah - IPC

Rod Rasmussen – individual

Martin Sutton

Caleb Queern

ICANN Staff

Margie Milam

Marika Konings

Glen de Saint Géry - GNSO Secretariat

Gisella Gruber-White

Apologies:

Jeff Neuman - Registry constituency

Greg Aaron: Please do. Thank you.

Gisella Gruber-White: Good morning, good afternoon, everyone on today's call. We have Greg Aaron, George Kirikos, , Roland Perry, Faisal Shah, James Bladle, Rod Rasmussen, Martin Sutton and we also have Caleb Queern.. From staff we have Marika Konings, Margie Milam, Glen de Saint Géry and myself, Gisella Gruber-White and apologies from Jeff Neuman. Thank you. And Berry Cobb has just joined as well.

Greg Aaron: Thank you. I see some people are on the line, most are in Adobe. We will be using Adobe today to look at some documents and so forth, so if you do have the opportunity please do log into Adobe Connect.

Before I go through today's agenda, just some housekeeping items, the first is a reminder that in addition to the recordings these calls are also put on transcripts. And occasionally the person who's doing the transcription has a little trouble figuring out who is speaking. They don't always know the voices by what they sound like, so a friendly reminder please do identify yourself if you haven't already been identified by name when you're speaking.

Also we have three Mikes in our group, so we're going to use Mike to mean Mike Rodenbaugh, Mikey to mean Mike O'Connor and then we have Michael Young and he'll be Michael. So that's how we'll do things, make sure the transcripts are attributed.

Also I'd like to introduce a new member of our working group, that is Caleb whose joined just recently and he's put up his statement of interest, but Caleb if you could just please tell the group briefly about who you are and your interest in the group.

Caleb Queern: Hello, everybody. My name is Caleb Queern. I'm the Chief Scientist at (Sivelance) in our Cyber Intelligence division and (Greg Overack), who I believe most folks on the call probably know, introduced me to the idea of joining and it sounds interesting and I'm excited to assist in whatever way I can.

Greg Aaron: Thank you very much, Caleb and we're glad to have you with us.

Caleb Queern: Okay, well today we'll do our usual review of the subgroups that we have underway and then we will move on as time allows to new topics on our list of potential abuses.

So first item is an update from the cybersquatting group and I think maybe - let's see - who is on board today from that group? James and...?

James Bladle: Probably just me I think or Mikey.

Greg Aaron: Actually I don't...

Mike O'Connor: This is Mikey. I'm not on that one. Sorry, James.

James Bladle: Okay, sorry.

Greg Aaron: I think it's just you James.

James Bladle: Once again - this is James and once again I'm standing in on this group, although I wouldn't consider myself a necessarily active member. The message that Mike posted to the list relative to some of the definitions of cybersquatting, we have not actually met as a sub team and there has not been a lot of activity other than the teleconference.

At this point I would like to post a suggestion that we - or at least take the position that we borrow the definition of cybersquatting as it currently exists in the UDRP and I think that, that idea has floated on the list as well. There are some interesting other definitions floating around out there, but I think that just from a personal perspective there's some - each one may introduce just as many complications as it resolves.

So I think, you know, for the sake of conformity of context within ICANN I think the UDRP definition is probably works for all purposes.

Greg Aaron: Okay.

James Bladle: And you know, certainly open to thoughts or corrections on that.

Greg Aaron: Okay, since the other members of that group are not on the call today would you like to post that idea up to the list where they can see it?

James Bladle: I think it has been posted Greg, but I will certainly, you know, post it in its own thread. And I will do that, yes.

Greg Aaron: Okay. Now another thing that we've done to try to assist you guys in this group is Marika has gone through the transcripts and did extract some information at the request of Mike Rodenbaugh, so she has posted that up to the list as well. I think the idea there is that's some raw material that came out of the discussions, but then the subgroup has to decide how to use that material and what to put forward or what to cut out of it, etcetera.

Marika Konings: I've posted that information as well on the Wiki for your information.

Greg Aaron: Thanks again for doing that, Marika. That was very...

Marika Konings: No problem.

Greg Aaron: So we've got some raw material up there and I think what we're looking at now from this group is to shape that material and continue to produce something, you know, get to something that the wider group can take a look at. I see George's hand.

George Kirikos: Yeah, George Kirikos speaking. I just wanted to support that we just speak to the UDRP definition and try to embellish it with other material. Just looking at the Wiki that Marika created, it still has a problem that arose last time or maybe two meetings ago, where it says, de-registration or acquisition of multiple de-meanings, which you know, are identical or confusing similar to marks of others that are distinctive at the time of registration of such de-meanings. That captures basically anybody who owns two dictionary word domains, you know, when its taking the position of what constitutes abuse, but what hasn't included all exceptions to that, you know, what excuses you

from being captured by that definition, so that's why we have problems with, you know, adding to it without taking into account all the other VI exclusionary aspects. That was point number VI in the Wiki.

Greg Aaron: Okay.

George Kirikos: And a lot of people do on more than one dictionary word domain that we use to people on this call alone and they're not cybersquatters, far from it.

Greg Aaron: I see Mikey O'Connor is in.

Mike O'Connor: Yeah, George just beat me to the punch I'll take my hand down. Sorry, same comment.

Greg Aaron: Okay and James?

James Bladle: Yeah, I think George is correct and there is also another point that - are we looking at the...

Greg Aaron: ACPA

James Bladle: ...ACPA definition here? What's on the screen currently?

Greg Aaron: Well that had been discussed by the group a bit.

James Bladle: The ACPA, yeah.

Greg Aaron: And we need a recommendation about whether we should do that or now, it is as you said, others - it's from another set of laws, it's from something different than UDRP.

James Bladle: Right and two - this is James again, and the two points that I think I posted I did not receive response was similar to what George was saying. That there's

a notion of (resuitism) or pattern behavior in the ACPA and there's also - it broadens the standard from identical string, which is what's compared under UDRP into choosingly similar, which I think has its own host of issues and complexities. So I think that, you know, that's just adding support to what George was saying about just going with what we have in the UDRP for now.

Greg Aaron: Okay, any other thoughts on cybersquatting for now? I don't see any hands raised. I'd like to move on, because I think where we are right now with cybersquatting is the group needs to make some progress using its Wiki and the recent material that Marika has provided. So I will, unless there are any other comments, let's use the cybersquatting group to its work and we look forward to seeing something from them.

Marika Konings: Greg, can I just make one comment? It's Marika.

Greg Aaron: Please do.

Marika Konings: No, I just wanted to offer to the group if there's any need to set up a conference call, so the group can actually discuss by telephone, you know, we're happy to facilitate that and they can just drop me or Glen an email so we can set it up.

Greg Aaron: Absolutely and of course that's something we're also doing for the Contracts group and if a group does ever need to block out some additional time for itself to get together the staff is always happy to facilitate that.

Okay, let's move on then to the next thing, which is uniformity and contracts and there's been a lot of work that's been done on this topic over the last couple of weeks, so I would like to turn the floor over to Barry, who's been doing some intense work on this.

Barry Cobb: Thank you, Greg. Yes, this is Barry Cobb. The shorten brief, we met again, excuse me, we met again last Thursday and had a pretty good session.

Again our charter more or less is to determine if uniformity of contract relative to abuse is necessary or not in our world or across the market place, before we can start to lay down recommendations or thoughts in that regard we needed to get a better idea of what currently existed out there today and so the team is working to develop a picture so to speak for us to gage the dispersion and/or variance across publicly available registration - registrant contracts at the current moment.

So that the research matrix that we're building right now - we started off with the top five registrars and we're reviewing through those contracts and tagging components that touch on the topic of abuse and were - our representative's sample will come - we made the decision that we shouldn't just review the top tier registrars, but we should also review middle tier and lower tier registrars and look at all their information.

So we're hoping that by next call, which will be sometime next week, either next Wednesday or next Thursday, that we'll have a representative sample across the registrar spectrum of what these - this dispersion in variance looks like. And depending on the outcome of that, there's basically kind of three paths that we anticipate that we might have to take, excuse me. The first path is that based on our research we see that there is quite a bit of uniformity and that we may not need to do anything at all.

The second path is that there is some variance in dispersion and some sort of recommendations might come out of that or the third path is that there's great dispersion and variance and a different set of recommendations may come out of that. We don't have a view as to which one of those paths will traverse, but again when we meet late next week we should be able to have a very good picture of what that dispersion looks like and then we'll come up with our action plan from there. And anybody else that's on the sub-team is welcome to comment in if I left anything out.

Greg Aaron: James, I see your hand up and I'll get to you in just a second. I have a couple of questions for Barry, just to kind of set the stage. So right now you're looking at the registrar contracts and notice - and basically tipping off in a variety of categories what this registrar does or does not have as far as its registrants. Now one - I guess one question is do all the registrars have everything in their RAAs, that they're suppose to have according to ICANN? So is that something you're looking at?

Barry Cobb: Not specifically. I guess the other comment I'd like to make is I'm hoping that after our team accepts the second slice of research that will make that available for the Wiki for the rest of the working group to see where we're going with this.

We didn't want to share it right now, just because it's very far from finished and it would raise more questions or concerns than answer anything. So I don't want anybody to, you know, I don't want you to think we're just trying to hoar) our work. I just wanted to make sure we have a very good finished product before we promote it. Excuse me.

Greg Aaron: Okay understood. It's still in a draft form.

Barry Cobb: Yes, so with that said we are focusing on just the abuse aspects of it, but going through the work I'm realizing that there is some very common sections that are across at least the top registrar documents and we're going ahead and tagging those that are even kind of outside abuse just to help establish some sort of baseline and to help build that uniformity picture so to speak.

There's also - the reason why I'm kind of going down this road is there is also some areas that touch on the post expiration domain name renewal working group as well and so, anyway there's kind of like a little bit of additional work going on to help build this picture.

But to answer your question, Greg, I wouldn't say that we're specifically checking off whether these contracts follow the RAA to the (tenth) degree, we're only really just trying to focus on anything that deals with abuse and additionally the scope is literally any kind of language or grievance or contracts that's publicly available on a registrar site.

So if a registrant contract doesn't touch or doesn't talk about a specific kind of abuse, we're also looking at like terms of use or universal agreements or other kinds of items outside of just a registrant contract. So we're trying to be as comprehensive as possible and just for the good of the group we're tagging this in two ways.

First and foremost is that we're looking for anything that has a formalized section within the contract, such as like an UDRP section or suspension of service section, etcetera, but we're also doing a review in the contract for specific abuse types. So, you know, we have our working list definitions that we're building right now.

We're also kind of just trying to peer into some of these contracts and do they say anything specifically about malware or Botnets? Do they say anything about (falsatives) or anything along those lines and we have the understanding that these abuse types and definitions are work in progress, but we just wanted to see what some of these, you know, what some of registrars were doing out there and if they were specifically identifying and building language around any particular type of abuse.

Greg Aaron: Okay. Thank you.

Barry Cobb: That's where we're at.

Greg Aaron: I'm going to recognize James, and then after that Mikey. So James please.

James Bladle: Thanks, Greg. This is James and I just wanted to support a lot of what Barry was reporting. A couple of quick points, there is an event later this week up in Toronto, so I apologize that I will not be able to attend the call if by next week statement you meant this week, Barry, I'll have to issue my apologies for that.

And second we did introduce a concept and maybe it's warranted in bringing it in front of the larger group where we discussed. The idea is uniformity always desirable or is non-uniformity always bad? And we certainly didn't make any judgments on that particular case, but we wanted to possibly discuss that in a wider audience when one considers the variety of jurisdictions and business models of registrars in the markets that they are targeting, so we wanted to put that out as well.

Greg Aaron: Okay. Mikey?

Mike O'Connor It was frustrating having my hand up later, because you guys all say the stuff I want to say. I think the only thing I want to add two points. First point is I think this going to be my ritual add a point for Barry, every time we are on this group call, because Barry is doing fantastic work.

The second is I just want to amplify a little bit something that Barry already said, which is that we are really doing sort of exploratory work right now to see, you know, we've kind of coined this term dispersion. We want to see how much variation there is, both between registrars, but also now between sort of tiers of registrars and the location of them, before we decide which course to follow and Barry has been fantastically responsive in changing the way that he's doing his research.

Partly we're doing this, so that we don't bury him with the analysis of 90 plus sets of contracts, but, you know, we started him off down the road looking at 10. At the last call we backed that off to five, but then said do five in the middle size tier and five in the smallest tier of registrars and by the way make

sure that you've got a little bit more dispersion in terms of where the registrars are located.

And Barry has been smoothly fielding all of those late breaking contradictory requests with very good humor and doing a fantastic job. So when we get through this next call is when we're expecting to be able to sort of plot our course forward and figure out A, whether we have a problem at all and then B, if there is, you know, a dispersion what the implications of that are.

Greg Aaron: Okay. Margie, do you have your hand up?

Margie Milam: Yes, I do. I wanted to clarify the RAA language that we were talking about a few minutes ago, if it helps at all when they're doing their research.

The RAA there's a section it's 3.7.7.11 and it's something that it goes into the registrant agreement and it indicates that the registered name holder shall agree that its registration of the registered name shall be subject so suspension, cancellation or transfer pursuant to any ICANN adopted specification or policy or pursuant to any registrar or registry procedure not inconsistent with an ICANN adopted specification or policy to correct mistakes by the registrar or registry operator in registering the name or two, for the resolution of disputes concerning the registered name. So that's the language that's currently specified in the RAA.

Greg Aaron: Okay. Barry?

Barry Cobb: Yes, Mikey, I just wanted to piggy back on what Mikey was saying and he is correct in terms of how we've kind of expanded our data points if you will. Just to clarify, you know, we talked about top, middle and bottom. What we're using as our reference as to who's in the top, middle and bottom is the number of domains registered by registrar according to (web hosting dot info), so traversing that list its very easy to take the top five and ten as there

the ones that predominantly own most of the market space and in terms of trying to get to the middle and bottom tiers.

This is kind of a new update that I haven't shared with our team, but it's not as cut and dry as that. When we start getting into the middle and bottom tiers we start running into some that I'm picking are - turned out to be resellers from another registrar, so we're kind of throwing those out as independents if you will.

And certainly when we get into the bottom tier its definitely not the bottom, bottom. You know when we get into the last 200 most of those registrars have less than 2000 registered names. So I've kind of bumped it up a little bit and anything that is - any registrar that is a little bit greater than .5% of the market space and/or more than 20 or 30,000 registered names that's kind of the space that I'm picking from so to speak.

So what we'll - we'll still have a very good representative sample across the entire the spectrum, but it's not as hard, concrete, middle or bottom tier. And then the last point is most definitely we are expanding the spectrum and making sure that I try to get a representative sample from the various countries across the world as well. Thank you.

Greg Aaron: Okay. Thank you. Thank you. Any other questions for Barry and his team? I don't see any. So Barry, you mentioned that you'll be having another meeting and then do you think after that you - the spreadsheet might be in shape where you're far enough along to share it?

Barry Cobb: Personally, I would say yes, but I would like agreement from the rest of the team. You know, we are kind of advancing down the road of comparing from one registrar to the next and I want to make sure, you know, there's definitely sensitivity around that, so before we share it and anything beyond our sub team I'd like us to make a decision as to whether we should maybe remove registrar names and those kinds of things before we share it openly, but I

think that we'll be able to bring conclusions to those kind of decisions at our next meeting and then whatever we decide. My hope is that we are in a position to share what we've got so far.

Greg Aaron: Okay great. Okay well we look forward to hearing more. And then I had a couple last questions. One of them is, it sounds like you're tracing language as far as it needs to go, because some of the registrant agreements that the registrars have also reference other terms and conditions sometimes, so they might not be in the registrant agreement, but it might still be binding on the registrant. So it sounds like you're tracing those. Is that correct?

Barry Cobb: Trying to where possible. You know, I can't say that I'm going to hit it 100% for every registrar, but that is my intent. And I'd also like to throw out there just real quick and Marika reminded me of this is our spectrum isn't going to just close with registrant or registrars. We're still going to, you know, eventually our goal is to try to scrub other documentation out there as it deals with the registries and those kinds of things as well. We're just starting at the most publicly available and accessible information at this point in time.

Greg Aaron: Okay. Sounds great. Okay, so anyway last call on this topic for today. Any other thoughts? And hearing none let's move on to malware and Botnet Control and that is Rod and myself. Rod, I don't know if you noticed, but late last week I did some editing on the Wiki.

Rod Rasmussen: Great.

Greg Aaron: So we've made some progress. What we're - one of the things we're writing about right now is we're going the background section and kind of the problem statement, which is pieces of malware like Conficker and (Torepig) that are controlled through domain names and one of the problems is that sometimes they use lists - malware uses lists of domains which may or may not be registered.

So you have the problem of some names might already be registered by someone and it might be the bad guy or it might be by coincidence an innocent party. And then you may have tremendous numbers of domains that could be used to control the malware, but aren't registered yet. Rod had pointed out some good background research that's been done on the topic and so I've been putting that material into shape and extracting some key quotes from it.

For example there is an estimate of the amount of money one would have to spend in order to register all the Conficker names. That could be used to control the Conficker Botnet and it's upwards of \$71 million U.S. So we're making a little progress there. I'm contributing, because I actually had to deal with Conficker this summer, because it was going to use names in some of the registries I work with. So Rod, any other thoughts on this one?

Rod Rasmussen: I have a little bit to add more than what I did a little while back. The only other thought is that I do - I did hear we have some new blood or fresh meat who might be able to add some expertise right to this very issue.

Greg Aaron: Caleb, I think he's talking about you.

Rod Rasmussen: I would be talking about Caleb, yes.

Caleb Queern: Hi, guys. I have to admit I'm going to be a little bit less than available I'd like to be for the next few weeks, but I'm happy to jump in right after that. I'm going to be getting married this weekend, so when I return I'm all yours.

Greg Aaron: Well that is the best excuse I have ever heard from a working group member anywhere.

Caleb Queern: Beat that.

Greg Aaron: That's wonderful. Congratulations.

Caleb Queern: Thank you, guys.

Greg Aaron: What are you doing on this call man?

Caleb Queern: Exactly.

Greg Aaron: Absolutely. Why don't we hook up in September and our very best to you.

Caleb Queern: Thank you very much.

Greg Aaron: As you take this next step. So that's great. Thank you. I'll tell you what in early September, Rod and I will contact you and we'll tell you what we're up to and why don't we talk about the additional background that you might have.

Caleb Queern: All right. I look forward to it.

Greg Aaron: Okay. Excellent. Thank you, Caleb.

All right. Front running is our next topic and George had volunteered to take the lead on that and George has been producing some material. So the floor is yours George.

George Kirikos: Hi, George speaking. Yeah, about eight days ago I went through and summarized all the discussions we had in the prior conference call and also discussions on mailing list and it's all on the Wiki for people to review and hope everybody had a chance to review on it. Start to review it. There hasn't been much discussion on the mailing list since that time, so I don't know whether there's anything more that needs to be discussed or whether people are prepared to start filling out those sections on the spreadsheet as to legitimate use, requires DNS and potential recommendations.

I already kind of went forward with some possible recommendations, basically reiterating the SSAC reports, but perhaps people violently disagree with me or who knows, so I kind of leave the floor open and welcome your input further.

Greg Aaron: Okay. And of course one of the interesting things that's happened recently is ICANN did release some numbers about the results of the ad - the new ad grace period excess deletion fee, which was instituted in April in most registries. So we now have some numbers from April and May and June. It appears that, that policy is having a significant effect and I forget if we circulated the link to that study or not. If not I can do it.

George Kirikos: Yeah, we did.

Greg Aaron: Yeah, okay. It basically says that, that's cutting down significantly on tasting, so a side note there. George, did you want to...

George Kirikos: I think Marika had her hand up first.

Greg Aaron: Go ahead.

Marika Konings: Yeah, no I just wanted to point out in relation to the elements study on fund running I have already forwarded the questions that were posted on the list and some of the discussion points and we expect a response from (Benjamin Aidelman) shortly on that. If there are any further questions on the specific study itself please do forward on to me, so I can coordinate that and in turn maybe we can get some feedback for you on that.

Greg Aaron: Marika, what are the questions that have been asked thus far?

Marika Konings: From this group or...?

Greg Aaron: Or well I guess from this group and in general, what are the questions that you are pursuing answers for?

Marika Konings: They are also listed in the Wiki page that George created. There were some questions regarding the methodology raised by Jeff. I think George made some comment, as well as James and Roland. Some were more general comments and I think too the links are there to those different, you know, threads. So I forwarded that and I said, if there are any - I haven't seen any other questions from other directions. There might be more, but I'm not aware of those.

Greg Aaron: George and then Mikey please.

George Kirikos: Yeah, I just want to follow up on that interaction between domain tasting and front running. There is some overlap as you suggested, for example, the way network solutions was doing the in discriminate front running of all names that were - all unregistered names that were left at network solutions, but the topic is bigger than just that.

You know, people had actually looked up high quality names that the front runners took and held on to, you know, more than just the ad grace period, i.e. they kept it forever or at least one year, then it wouldn't be caught by those statistics that I can produce on domain tasting. So that study, you know, just covers one aspect of the interaction between front running and domain tasting.

Greg Aaron: Okay. Mikey?

Mike O'Connor: This is Mikey. I confess that this is the very first time that I've looked at the Wiki page and it's looking great. I'm curious George, if the bottom possible recommendations - are those ones that you came up with or are those ones that we talked about on the list. Tell me a little more about those. I like them. I'm just curious.

George Kiriknos: Those are ones I came up with on my own, that's why I put for discussion. And there hasn't been very much discussion, but I'd be happy for everybody to discuss. There are some that I'll probably disagree with them like (Jeff Eman) as a registrant might not be in favor of some of them, but I thought I'd toss them out there just to discuss.

Mike O'Connor: You know, I would encourage other folks on the call if you're like me and haven't looked at the page to take a look at those. I think they're (substantive) and useful for discussion and so I think Greg you may have to crack the whip over us to dive a little deeper on that one.

Greg Aaron: Okay. Consider it cracked. And George is doing exactly what he should be doing, which is, you know, putting stuff into that template, you know, to get material out in front of everybody for consideration. So drafting recommendations and so forth, that's absolutely what every group should be doing.

We will eventually, you know, we can discuss those offline on the list of course and then eventually we will go through each section for each topic and talk about them more formally, but I'm always very happy to see anybody putting stuff down on paper, where everybody can see it and think about it.

Mike O'Connor: This is Mikey again. I just want to support that. I've worked on - outside of ICANN a lot of policy stuff and it's always really helpful to have a draft to work from rather than having to come up with it from a clean sheet, so I didn't want to imply at all that I disapprove of what George is doing, quite the opposite.

Greg Aaron: No and I didn't take it that way. It's - I just want to continue to encourage everybody to do what people like Barry and George are doing. That's our goal to get that stuff out there. Get something down for everybody to think about. So George?

George Kirikos: James had his hand up first.

Greg Aaron: I'm sorry. Go ahead, James.

James Bladle: Thanks and this is James. And that is great work George. I just wanted to point out that's a really great synopsis of a lot of different materials. And I wanted to point out that if it is not currently in your list we could add it or if it is there and I haven't found it yet perhaps we can highlight this idea, but, you know, as a registrar when you're offering domain registrations online a lot of things can happen during a transaction.

So you know, very legitimately someone could look up and purchase a name, but then the credit card has expired for example or their browser crashes in the middle of a transaction and we wanted of course to provide a way for the customer to recover that transaction and finish it properly. And I think that that's sort of a genesis behind some of these ideas of what's called a cart hold. I don't know that they - since the change in the (chasting) policy, HEP restrictions,

I don't think that we're seeing this product or service quite so much and I'm the only registrar on the call and we don't do it, so I'm just kind of throwing this out there to the general community as this idea that - is there any legitimacy to someone coming in registering a name and the registrar putting it on hold for that person, as long as that specific person who actually did the initial look-up and registration is able to recover that name and that is separate from what we would traditionally think of as front running.

Mike O'Connor: This is Mikey. I'd really like to see an exploration of that topic, because I've always wondered what happens in the middle of a process that could take 5, 10, 15 minutes, how the ties, if you will, get broken and I think it might be something very useful to explore or make a recommendation about and set

some rules of the road for the registrars and registrees on this, so I'd second that motion.

James Bladle: And this is James again. I'd like to point out that the cost justification or the economic case for offering such a service is probably evaporated with the restrictions in AGP. So this may be irrelevant in the current context, but it certainly wasn't a couple of years ago or this time last year and I just wanted to put that on the table for consideration as we try to put some boundaries around front running and especially some of the legitimate uses of what could be, you know, tarred with a front running brush and also possibly some of the failure cases of registration processes that might look like front running, but they're in fact breakdowns of that system.

Mike O'Connor: This is Mikey again. I think the substitute I'd offer is registration of topical domain names. So you have to sniff 54 group tiers on the scene and/or, you know, the scientific concept of (argobarg) and two people or more simultaneously try to register the name, what happens if person A started the process at 10 o'clock sharp, person B came in at 10:05, person A's browser crashes and they don't get back to the session until 10:10, who wins that tie and how is that decision made I think is a really interesting topic.

James Bladle: So race track conditions.

Mike O'Connor: Yeah.

Greg Aaron: This is - yeah - this is Greg. So James are you kind of talking about where a registrant is actually trying to register domain name and then they - their browser crashes or whatever while there in the sign up process. It's not that they just have looked it up. It's that they're actually trying to buy that one?

James Bladle: Yeah, it's that it's for - if I can use some very non-uniform language - it's basically it's registered and its put into their cart, so its been - the avail check

has been sent to the registry. The create command may or may not have been sent to the registry, depending.

Greg Aaron: Registered domain name. And then they - their browser crashes, or whatever while they're in the sign up process. It's not that they just have looked it up. It's that they're actually trying to buy that one.

Man: Yes, that it's for - if I can introduce some very non-uniform language, that basically, it's registered and it's put into their cart.

Greg Aaron: Mm-hmm.

Man: So, it's been - the (avail) check has been sent to the registry. The create command may or may not have been sent to the registry, depending upon at which stage in the transaction the registrar executes that. Now, to add to complexity of what (Mikey's) example there, suppose Registrar A for the early bird that wants to get the domain is very conservative and doesn't issue the (avail) check until - or the create command until after they've been paid. Suppose Registrar B is a little more aggressive and enters it while the customer is entering their credit card, figuring that you know, they can play the odds that 99% of those transactions are going to go through.

So you know, the racetrack conditions definitely enter into this as well as the failure conditions, during the registration process.

Greg Aaron: Mm-hmm.

George Kirikos: George here. Just to go over - I think this might have been discussed slightly in the SEC reports, and that's probably one of the recommendations of this being a better education. What it's come down to really, is how registrars design their (prophecies). You could have one registrar where the order don't take - well, where the user, you know, registers online - registers their credit card, and then does availability checks, kind of like Amazon's One Click.

And if you did it that way, then there really is no issue about delay, because you don't even bump - a proper design wouldn't even do its availability check to the registry. They would do the registration - the availability check locally if they had a copy of the zone file, or if they had a copy of all registered domains. I don't know if people caught on to that discussion, but if registrars are better educated, they would design their registration process with these kinds of issues taken into account, and they can do that, you know, competitively.

One registrar, (Who Is) you know very security conscious, wants to make sure that nobody else can get access to their information, will never query the registry. They would just issue a create command, and they'll issue that create command after the user has logged in and so on. But (unintelligible), if we do suggest like a card hold, that just you know recreates the loophole that people can take advantage of, so I'm not sure that people want to go down that road.

I can mention it more explicitly in the Wiki, but that's how I personally feel, that if you implement the card hold, it's just creating the - another grace period that people will abuse, and use that as an option instead of an actual, you know, committed purchase. And in fact, the data purchased took place like on a One Click, that's something that the registrars can implement competitively like this, you know, your ICANN policy.

Mike O'Connor: Hello, this is (Mikey). I'm entrenched with process stuff, as people who've worked with me before know. And I think that one of the things that's useful about just mapping out the process with the various transactions going to various places, the authentication, the authen check versus the - I'm not even using the terms because these are all new, the (unintelligible). It seems to be useful to get those sort of out into public view, and have a conversation about things like how long a period of time, for example, should a card hold be permitted in some, if permitted at all. Ten minutes? An hour? A day? As the

time goes up, I agree with you George, that's where the front running kind of issue - or the issue with (unintelligible) starts to reappear.

So, I'm not sure I know where I stand on it. I'm mostly just lobbying hard for exploring and documenting at this point.

George Kirikos: George here. There actually would be a way to do it if one wanted to do it properly, and that would be to just for short periods. And secondly, I mean if the (meaning) doesn't resolve because the (add grace) period as it currently stands, you can add the name servers, test the traffic; make sure it's a good name in that sense. If you remove the ability to have the name resolved, then the registrar - sorry, the front running registrar and whatever, the - whether that is the registrar or some other person can't check to see whether the name is getting traffic, and figure out whether it's you know, economically viable domain name on its own. That would be one, you know, compromise.

Mike O'Connor: Yeah. This is (Mikey). That - you know, it's that kind of stuff that I think if we sort of dissected this process a little bit more, documented it, you know, we (authenticated) that in some of the inner registrar transfer, thus if we can sort of take that process apart and put it on the table, then that's where some of these ideas sort of can quickly be suggested and wind up...

James Bladle: Hey, (Mikey), this is James. I'm sorry, I tried to put my hand up a couple of times, and it keeps veering.

Mike O'Connor: I'm sorry. I'll be quite now.

James Bladle: Oh, that's okay. I just wanted to jump in and say you're tracing very closely, if not wading right into what registrars consider the recipe for their own, you know, secret sauce in some of these processes, you know. And it really boils down to, you know, some things about risk tolerance or experience with different customers. As George was saying, we have certain customers that you know, we have - we allow them to keep methods of payment on file.

Some registrars would feel that it would be perhaps too risky to accept credit card or online payments at all.

So, you know, I think that documenting the process would be interesting, and would definitely help perhaps bring some of the, you know, the alleged ideas about front running out into the open. And I think would probably vindicate a lot of the folks that are continuously tarnished with that idea. But ultimately, I don't think that we're ever going to get that kind of a peak behind the covers. And again, I'm not trying to be an obstructionist here, I'm just trying to say that you know, we're started to traipse into an area where registrar support is very hard and become very innovative in developing these processes.

And there may not be a one-size fits all for all different types of customers. And you know, leveraging that knowledge for a competitive gain versus their - versus other registrars is very important to all of them.

Man: Okay, I see.

George Kirikos: George. That's right. That's why I said it's kind of like an education issue, that the registrars might not necessarily want to participate in because it might give an advantage to their competitors. But, it was kind of already caught up in the SEC reports. If you look at the Prior Research section, it says, "Checking the availability of a domain name can be a sensitive act which may disclose an interest in/or value ascribed to domain names." Then, it talks about third parties, because you know, the way for example I register a domain name, I you know, am very sensitive about how I do a look up because I'm, you know, paranoid by nature I guess about domain names and their availability.

But, you know, if you go to certain registrars, they'll you know, run that name through multiple means spinners, they'll give you names that are available for sale in other market places. So, there's all kinds of leaks to third parties that can take place. And ultimately, the registrars are able to compete on the

basis of how much they disclose to third parties, and so on. So right now, we do have a level playing field, but the actual (place) that I was most concerned about is at the registry level. Because of all the registrars are able to compete equally, the registries do have ultimately the most sensitive data. And if there was a policy that needed to be created, it might need to be directed mostly to them, but...

Mike O'Connor: So, this is (Mikey) again, and I'm sorry I don't have my hand up, so Chairman Greg, shove me up any time I'm going too far.

Greg Aaron: Hey, (Mikey), go ahead.

Mike O'Connor: Is that a yes I should shut up now?

Greg Aaron: That's...

Mike O'Connor: Let me do one more round. It seems to me that the way through this is maybe to stand firmly on (George's) education island, and educate - you know, draft a process not by asking registrars or registries to reveal their particular practices, because I get that secret sauce stuff from (James') point. But rather, to go back to (James') earlier part of this conversation where he was sort of laying out the different possible ways of doing it without saying who does what, and then kind of play the either education opportunities or policy opportunities that that generic discussion produces.

I think that the good fight here is to find a way to have that conversation without impinging on the proprietary processes of registrars, because this little piece of this call has been very enlightening to me. And I'm sure that there are lots of less sophisticated registrants who would also benefit from understanding those issues. So, and now I'll this dog lie.

Greg Aaron: Okay. All right, this is Greg. I had my hand up. And I guess as usual, as any topic that we're exploring, we need to put - to establish what the harm is or

the damage - in other words, is it an abuse or not? So, as we get into the niceties of what registrars are doing in their implementations, think about that. And George, I see your hand is up.

George Kirikos: Yeah, I cleared it, but it was still up. You know, basically, I guess the harm really is to people that are not educated. Like people that are first time registrants, like the grandmother in Wisconsin that wants to, you know, get a domain name for her blog, and she has a bad experience registering a domain name because you know, somebody will take that. The harm I guess isn't to the registry, because you know, the domain name still gets registered; VeriSign still makes their seven bucks, whatever. The registrar still makes their profit. I guess it's the turn off effect, because they don't know any better. You know, the uneducated, or the (UB) consumer, so that's why it's lot of my recommendations - or a lot of the recommendations that I put in the draft were education and how to do that, and disclosure by registrars.

And then Number 4, I guess was disclosures is filed, the registry is more studied. Number 5 really, is going to sophisticated people, if you have that list of all registered domain names, then you don't actually have to do that availability check. So that, you know, helps registrars themselves raise the bar on how they do availability checks. It reduces that information leakage that can occur. And so I guess, you know, the sophisticated user are never going to be harmed because they know all the rules inside out. It's like it's the unsophisticated ones that are potentially turned off by the process. It might not be you know real harm, because they never had a right to a certain domain name to begin with.

Greg Aaron: Okay. Okay, any other comments on where we are at the moment on this topic?

James Bladle: This is James, and very briefly, just wanted to say George, there are numerous problems checking the zone file, as you mentioned, versus

sending the availability check, and we can discuss that offline. But, just wanted to maybe point that out, and we can move on.

Greg Aaron: Well, it sounds like an action item for everybody is to take a look at the work that George has placed on the Wiki. Ask him any questions or make any recommendations or changes that you would like. And as Marika had mentioned, if you have any questions about the (Adleman) study, you can send those to her, and she has put the questions of our - up on line.

Okay, we are at the top of the hour, so we have about 30 minutes. Does anybody need a quick break before the home stretch?

Man: No.

Mike O'Connor: I'm okay. This is (Mikey). Let's keep going.

George Kirikos: Good here.

Greg Aaron: Okay.

George Kirikos: We may even be finished early.

Greg Aaron: Well, we've - there's always more. If everybody's fine, let's go to a new topic then from our list. And Marika has that doc. She'll put it online.

After front running, we had another - a topic which was inappropriate use of (Who Is), but maybe we fold that into the bigger (Who Is) question. We will be referring (Who Is) up to the counsel in some way. I'm working on that right now. Just to try to get some clarity on the scope. So after that was use of stolen/fraudulent credentials. If memory serves, that was a topic that (Rod Rasmussen) was interested in . (Rod), though, has dropped off because it's early on the West Coast, and he's taking care of his kids at the moment. Does anybody mind if we circle back to that one later when he can join us?

Okay if not, what we - after that, we've got a set of -- for want of a better term -- perhaps crime related, and we may need to do a little consolidation around these. What we see on the list is -- let me pull things up here -- we've got phishing, and then phishing emails, malware, malware emails, phishing, email scams, and spam. I'm wondering if that really boils down to just three things, which would be phishing, spam, and malware; they're all in some ways related to each other because the way you get people to go to a phishing site is by sending them email. Some but not all malware is spread via lures in emails. So, I'm wondering if we should just say phishing, spam, malware are the three categories with some obvious interactions between them. But, they also seem discrete (unintelligible), so any thoughts on that?

Berry Cobb: This is Berry. I would take a position on consolidating these. Let's try to make it - you know, make it a little bit simpler.

Greg Aaron: Okay. I'll take it upon myself to provide some notes up to the list on that after we've heard all the comments. (Mikey), I see your hand.

Mike O'Connor: Yeah, sorry. I was away from my computer. I guess the question that - I don't remember how we resolved this. Could we come to a conclusion on the distinction -- this is a scope question...

Greg Aaron: Mm-hmm.

Mike O'Connor: All right, in many cases, that's not registration abuse, that's domain name abuse, and I can't remember where we landed in terms of whether those are even in scope.

Greg Aaron: Well, I think that is the next big question. We need to do some consolidation, because if we decided it's out of scope, we still want it mentioned in the report that we talked about the things that - I think if - you've opened up the next big question. Are these basically, registration issues or are these use

issues? Now first, we should make sure that everybody understands kind of the mechanics of how these problematic activities take place, and I've done a lot of professional work on these.

Pfishing is defined as a - basically, putting up a false Website that purports to be a financial institution or other kind of site. And the criminal puts up that falsified page in an attempt to get people to input their credit card numbers or other sensitive information. Some pfishing is done on Website pages where the domain has been registered by the pfisher. They need to put up a site, so they got to register a domain. About 20% of pfishing cases are on domains registered by pfishers, and that statistic comes from the semi-annual pfishing surveys that (Rod Rasmussen) and I do. We actually study all the pfishing that takes place over a six-month period, and we go through all the domains and so forth. I mean, we break them out.

About 80% of the pfishing sites are on compromised Websites. These are Websites owned by innocent registrants, but the criminals are able to basically hack into those through - because the Web server is insecure in some fashion, so they - the criminal does this for two reasons. One is free hosting. It makes it more difficult for them to get traced. So, you have some sites that are purposefully and maliciously registered, and then you have some domains that, you know they're just hacked and are being used unfairly, basically.

The next thing is spam. We are really familiar with spam. Domain names are registered in order to perpetrate spam. Some mails are sent from registered domain names, because you need to set up a domain name to send the mail from. Spammers also use domain names to set up a destination site, so if they're selling you - trying to sell you a service or product, they will sign up a domain name, advertise the domain in the spam to try to get people to go there. Pfarmering is basically a flavor of pfishing that involves redirection, sometimes through malware, but it's basically trying to get you to a faked site where people can steal your credentials.

And then malware, again, it comes in two varieties. Some domain names are registered specifically by bad guys to - as a place where people can go, and they'll land there and they'll get that malware downloaded to their machines. Or a domain can be set up as a place where the malware resides, but is spread from there to other sites. So again, you have maliciously registered sites which are owned and operated by bad people. However, in a lot of malware cases, evidently the vast majority, domains with malware on them are actually infected. And so, these are sites that have gotten the malware from somewhere else, again maybe a vulnerability in the hosting software. The registrant may not know that it's happening, and it is certainly not their intent.

Sites infected with malware in the past have actually included some very well known and trusted Websites, like newspapers or Walmart.com for example. Bad guys are actually able to insert things onto those sites in various ways. So again, you have two situations; maliciously registered domains and innocent or compromised domains.

Okay, so any questions on that stuff I just laid out? (Mikey), I see your hand up.

Mike O'Connor: Oh, I'm sorry. I didn't take it down. My apologies.

Greg Aaron: Okay. Martin, go ahead.

Martin Sutton: Hi, Greg. All I was just thinking, though, as you were going through this list -- I've just come back into the call -- but all of this sort of phishing and malware elements, as you were just mentioning at the end, a lot of these are where they're taken over at some stages, not to do the actual registration of the domain, but where they are used in phishing or deploying malware, and set up specifically to do so, it's highly likely that they're using false (Who Is), or not using valid payment credentials or stolen cards, et cetera. So, I think that gets

picked up, or should be picked up from some of the other work listed down for the investigating (Who Is), et cetera.

Because I think that's the primary issue here, that they're enabling the use of domain names for these purposes, because they still give the anonymity and - that frauds just want.

Greg Aaron: Mm-hmm.

Martin Sutton: So, I just wanted to raise that comment now, because I still think there's - some of the work that is included within this working group will have an impact on - or could potentially have an impact on these sorts of issues. But perhaps, not as direct as you would expect from the list here, so these may be questionable about whether they're in scope or not.

Greg Aaron: Okay, so to paraphrase, (Who Is) is a way that criminals obscure their activity, and domains registered for these kinds of bad purposes are often registered also using stolen credit card credentials. So, that's one of the issues that you're interested in. Is that correct?

Martin Sutton: Yes, certainly. Yeah.

Greg Aaron: Okay. (Mikey), I see your hand up still?

Mike O'Connor: No, now it's for real. This is (Mikey). I think that there's some sort of distinction we could draw between (Rasmussen's) example of domain names that are embedded in a botnet, but not yet registered. Clearly, that's domain registration abuse, because there is a plan to register domains for bad purposes sometime in the future. And that it seems to me clearly falls within the scope.

There are other instances, a lot of the ones that you described, Greg, where those seem like domain name abuse, and fall outside the scope of our

charter, which is the registration event. So, I wouldn't want to throw all of these out, but rather discover the ones that zero in on the registration process, but leave all of the other instances to some other working group; otherwise, we're going to be working until at least 2055 trying to keep up with it. So, I guess my - the point I'm advocating is, let's try and A, I agree consolidating is good, but then B, let's also try and be very careful of scope.

Greg Aaron: Okay, I approve. Martin, do you have additional comments?

Martin Sutton: No. No, not at this stage. I think (Mikey's) points are good. That don't - bury these ones out of the way at the moment. These - I'm just wondering whether we can have a look at some of these and put in specifically the fact that they are registered for malicious purposes, and then in that way it segregates those that are hacked into or abused post registration.

Greg Aaron: Okay. And George, your hand is up.

George Kirikos: Yeah, I'd echo the concerns of (Mikey) that one wants to make sure that we remain in scope. If we use an example of, you know how telephone numbers are allocated, you know, you would look at the allocation process, making sure that people have accurate information through their phone company (unintelligible). I don't think the SEC would consider the rules making rules about - to the content, or how the phone numbers are used. You know, they would leave that up to the law enforcement and other agencies of the government. They wouldn't do it through the registration of phone numbers aspect.

Greg Aaron: Okay. I'm going to raise my own hand. This is Greg Aaron, again. One of the questions that - we had a very related set of issues come up in the fast-flux working group, because the problem with fast-flux is not so much an issue of the technical practice. As it turns out, fast-flux is something that, depending on how you define it - that you implement it, it can be a benign thing or a bad thing. What we were really interested in was malicious use of fast-flux, and its

use by creating botnet to facilitate this, and botnets are clearly a bad thing. They're illegal.

One of the issues that came up was this issue of malicious registrations, therefore. And the issue became, how do you figure out someone's intent when the name is registered? And is that even a valid thing to do? With fast-flux the - you find out about it after someone has detected what's going on basically, which is obviously post-registration. In some cases, fast-flux criminals use the domain name very shortly after they've registered it. In some cases, they wait a few months. They let the domain age for one reason or another.

So, one of the key issues we wrestled with there was this issue of intent and basically, criminal use. We need to talk about this issue some more, I think. I see (Roland's) hand up.

Roland Perry Oh, yeah. Hi. I was just going to bring into the conversation the (IRT). I went to one of their road shows in London about a month ago. They seem to be saying that so far as they were concerned, almost the entire problem with abuse of trademarks and brand names, and so forth, was people obviously and deliberately setting up sites to sell counterfeit goods, and I suppose that would also include pfarming sites and pfishing sites.

And so on one hand, I think we got some people agreeing with my point of view, which is that a lot of these sites are set up deliberately. You can tell by the name because it relies on somebody else's brand name, but also we have a potential overlap here. We've worried in the past about overlapping our activity with another activity, and maybe all of these are going to be marked out by the (IRT).

Greg Aaron: Well, I think the (IRT) is dealing with a more limited scope, which is trademark issues, which are all - another way of saying that is civil issues. Now, what we have is actually a broader thing, which includes some criminal issues. (IRT) is

not -- as far as I know -- talking about phishing or spam or malware, or anything like that. They're talking about trademark infringement.

Roland Perry: Yeah, well we've got -- it's (Roland) again -- we've got like sort of a silo issue here, because we in the past have seemed a bit reluctant to talk -- for example -- about (Who Is) issues on the basis that somebody else is discussing that, but (Who Is) is a very narrow issue. It didn't seem to crop up then that we could also discuss it because it was a narrow issue. So, if the trademark abuse that the (IRT) is looking at is a narrow issue - you know, or maybe I suppose we can look at it, but we should also look at the (Who Is) in that case.

Greg Aaron: Greg again. I'll throw out an interesting fact. And like with the (IRT's) discussions, they're of course interested in CyberSquading, which means that the domain name is associated somehow with - for instance, a trademarked term or brand name, so the brand name is in the domain name itself in some way. In the cases of spam and phishing and malware, that may not necessarily be the case. I can point you to some research that (Rod) and I did, and it actually - the phishing cases, a very small number of the domains registered actually have the name of the bank or other relevant institution in them. Phishers just use whatever domain name they can get their hands on basically. In some cases, the domain names that are registered mean nothing at all. I'll post a link up to some of the papers. So, kind of different ways that people are doing, and carrying out these activities, I think.

I see (George's) hand.

George Kirikos: Yeah, I just wanted to give another example to kind of demonstrate the scope issue. If you looked at for example registration of companies, people, you know (unintelligible) individuals might want to register a company in order to avoid taxes, or to engage in all kinds of illicit activity, but their actual registration process of that company could've been you know, perfectly

legitimate. No abuse happened. You know, you catch them elsewhere, you know, in how they violate the law - the other laws.

You know, companies are fined all the time for criminal activity, you know, monopolistic behavior, but they don't (unintelligible) their corporate charter. That corporate charter might have been perfectly registered, so I just wanted to toss that out as another example, following-up on the telephone number example before.

Greg Aaron:: Okay.

Mike O'Connor: This is (Mikey). The pdf - or the Acrobat thing just went away for me. I don't know if it did for anybody or not, but let me chime in rudely, and then I'll get out of the way. I'd be interested in being in a sub-group working on this with the charge of trying to figure out those things that constitute registration abuse in that (triumphate) of bad things to do. That seems like a really useful exercise for us. And I just throw that out as a way forward.

Greg Aaron: Okay. That would be a next step, which is try to figure out what the scope issue is, whether it's in or out, or whether there are aspects that are in. I would be happy to join you in that, (Mikey). Do you want to take the lead on it, and I'll join you on it.

Mike O'Connor: I am not going to be able to do as great a job as Barry, because I'm in the last few months of a two year statewide broadband, and I'm writing my brains out, but maybe we can kind of nudge each other along, because I'm pretty overwhelmed at the moment.

Greg Aaron: Okay, well is there anyone else interested in tackling this subject? I'm willing to guess that (Rod Rasmussen) might, because he knows a lot about pfishing.

Martin Sutton: Greg, it's Martin here. I would like to also - yeah, I'd like to get involved in this one, in terms of there must be some impact I'm sure on registries and registrars for having to unwind a lot of this stuff without getting any revenue in from it. So, it intrigues me still. There's probably not a great deal of information flowing around as to work out what that impact is, and what proactive measures they employ to filter out any fraudulent activity. Because, they must have some experience from certainly the phishing data. I'm sure some have eluded to the fact that they do quite a lot of up front filtering to minimize the risk to them.

So, certainly I'd like to participate in that one, and see if there's anything from sort of the financial institution side that we can look at and explore within that as well.

Greg Aaron:: Okay. All right, so we'll add you to the group. So, that's you, me, (Mikey), and I'll - we'll ask (Rod), because he might be interested. Is anyone else interested in joining this sub-effort?

Okay, I don't hear any. Marika, it sounds like we can set up another Wiki for this topic. For now, I guess we could call it Phishing/Spam/malware, or something like that. I'll take it upon myself to post up to the list a way to consolidate these subjects that are on our master sheet. And let's go ahead and set up a Wiki with that tentative title for now. We'll assign (Mikey), Martin, and myself, and then whoever else wants to join us over time.

The goal on this Wiki is going to be to try to figure out the scope issues. For example, are there aspects of the - what aspects of these are in scope? What might be out? And do a little digging into the background. How does that sound? Okay?

Mike O'Connor: Marika, this is (Mikey). Could you also do the call scheduling (doodle) thing? It seems like it'd be good for us to get a call on...

Marika Konings: Okay, could you just indicate - would you like a call this week or next week?

Greg Aaron: I will be on vacation next week, for what that's worth.

Mike O'Connor: This week is fine with me. You know, I've got some gaps in the action. The earlier in the week is actually better. By the end of the week, I'm out of town dealing with this broadband (at this moment), so it would be great if we could do it either tomorrow or Wednesday.

Marika Konings: Okay, (unintelligible) is about to get a (doodle) going, and if not this week, maybe we can do it in two weeks time, otherwise.

Mike O'Connor: Yeah, okay.

Martin Sutton: This is Martin here. Wednesday is probably better for me this week, if we're going to try and do it earlier. That's good.

Marika Konings: We'll try some times on Tuesday/Wednesday. You can indicate what works, okay?

Martin Sutton: Okay, cheers.

Greg Aaron: Okay, great. Well, in one fail swoop, we've addressed - it looks like we gotten underway on several rows on our master sheet here, so that's good. We have just a couple of minutes left before we have to close things down. Just briefly, as far as scheduling, our next meeting is in two weeks; same time, same channel. And then, the week - let's see, the next meeting after that would be September 14. We agreed last time that those times were fine. That skips over the -- what is it -- the Labor Day Weekend in the United States.

So, are there any other closing comments from anybody?

George Kirikos: George here. Do we have a schedule of what we should do for the next meeting?

Greg Aaron: Yeah, I'll be putting out the action items from the minutes, but we've got some action items on each of the groups that we've gotten underway here, it looks like. I'll put those up to the list.

George Kirikos: Okay.

Greg Aaron: And then, if I've missed anything, please let me know.

So, thanks again, especially to those of you who've been working on material up on the Wiki, folks like George and Barry. That's really one of the big purposes of this working group, which is to get that material up for people to discuss and react to. The time that you're spending on it is very much appreciated, so thanks again, guys. Good job.

So, if nothing else, why don't we - we'll close down the call, and thanks. Please enjoy what remains of your summer. And we'll talk to you again in two weeks.

Mike O'Connor: Thanks a lot, Greg. Great job.

George Kirikos: Bye, everyone.

Marika Konings: Thanks.

Man: Thank you, everybody.

Greg Aaron: Thanks, everyone. You take care.

THE END