CR - RAA Progress Report and WHOIS Data Validation Workshop
Monday, March 12, 2012 – 13:00 to 15:00
ICANN - San Jose, Costa Rica.

NANCY LUPIANO: Good afternoon, ladies and gentlemen. We're about to begin our RAA and WHOIS validation workshop. Please welcome Volker Greimann and Kurt Pritz who will act as our moderators.

KURT PRITZ: Good afternoon, everyone. And thanks, Volker. This is really a bifurcated session. First, Volker from the constituency and I will provide an update as to the status of the RAA negotiations where we're seeking to amendment the RAA, the registrar accreditation agreement. The session is meant as a brief update. It will reflect the material in the status report that's provided, identify next steps. And then at the close of that we'll go into what we think is the most important and, frankly, very interesting part of this session where we have -- we -- the registrars and us and the committee -- have put together a panel, a very esteemed panel who is going to describe different WHOIS validation models for us. The effectiveness of them, the cost, the benefits.

So it's not so much a session to debate whether WHOIS validation or verification should be undertaken, but, rather, how. And this panel will present models to us. And I think it's going to be fabulous.
Since there won't be questions and answers about the RAA status here, if anybody wants an update in their constituency group or community group or other ICANN organization, advisory committee, we'll work to schedule that. So see Volker or Gray, as the chair of the constituency, or me. And we'll seek to arrange that session.

So we'll start with the RAA update.
So these negotiations and the proposed amendments to the RAA are wide ranging and seek to address a variety of interests. They include, very importantly, law enforcement agency recommendations. We also have a set of recommendations from the GNSO that's prioritized from us as far as high and medium senses of urgency. The ICANN board and staff and, in particular, the ICANN compliance group has a set of requests they would like to see for improvements incorporated into the RAA. And the registrars, too, would like to see improvements to bring

the agreement up to date to reflect the current market situation and to improve their ability to bring services to registrants.

Also included in the negotiations are topics to advance registrar protections and DNS stability. But I'll tell you, for the very few months we've been working on this, there's been a high priority placed on the law enforcement recommendations and ensuring that there are changes reflected in the agreement that correspond to every one of the law enforcement recommendations.

It's very hard work both from scheduling and time and for subject matter.
So, as far as scheduling and time, there's been over 12 meetings between the registrar accreditation negotiation team, which is called the NT, the negotiating team. One of the shortest ICANN acronyms ever.

There's a telephone conference every week. Progress is -- meeting notes are posted on the Wiki, and a status report is published. I'll say there's been some criticism about the amount of detail of the negotiating session posted on the Wiki. Early on in the process, we found ourselves negotiating what we would post publicly for a longer period of time than the substance of the negotiation. So we agreed pretty rapidly to the detail in the notes we have now. And we wanted to move forward on substance. But comments about that are welcome, and that can be changed.

So what makes this work so hard? There's been significant progress to date. The discussions are very constructive. There has been suggested amendment on every one of the law enforcement asks. When there has been a question about specificity of the law enforcement ask to understand exactly what the goal is, we seek to relieve that uncertainty by meeting with them. So there were two face-to-face meetings between law enforcement and ICANN in Washington, D.C. One of them included registrars.

The registrars themselves have met with law enforcement to get clarification. So we've read the words in the law enforcement recommendations very carefully. And, when there's questions, we seek to answer them. So one question was -- one law enforcement ask -- and here I'm paraphrasing, so this will be inaccurate in itself, but -- so the

registrar will post that they have a legitimate business license where they're doing business.

Well, in the United States would that be in the state of Delaware where they're incorporated, their principal place of business, offshore? So we got clarification from law enforcement that that's a pretty loose requirement. Where you're doing business, show us a license. Where we've sought clarity on WHOIS validation, we've gone back and received, you know, a reply from law enforcement that we're looking for complete, accurate information so we can find people, if we need to.

VOLKER GREIMANN: Maybe just as an add to that, it has been helpful to talk to the law enforcement community about the asks that they have made, because a lot of these asks are not seen as direct we want this in the contract, but rather this is something that we have thought of to reach certain goals. So focus on the goals of law enforcement community has been very helpful as well.

KURT PRITZ: Thanks. That was a good comment.

Where there's a gap between the law enforcement ask and a registrar offer and compromise, so far that's been identified as an area of non-agreement that the negotiating position right now is up against the law enforcement asks. So I wanted to let you know that, although negotiations continued.
We've spent the most time on the law enforcement 12 requests. As I said, the registrars have certain changes they would like to see in the agreement. ICANN has changes. We're also addressing the GNSO subjects that have been brought up.

What makes this more complex is that it's a negotiation. So each side doesn't want to post an agreement until the agreement is negotiated in full. So, if one side makes many changes -- I'll call them concessions -- they don't want to post those concessions absent some discussion about their asks. Neither side wants to give up leverage on the whole by publishing a partial agreement. That's why the publish status is not as certain as it might be with respect to the agreements that have been made between ICANN and registrars.

Given this complexity, we've worked to write a complete agreement so there exists one whole agreement with changes that address the many recommendations. And that's being passed back and forth between registrars and ICANN and redlined by each side. So that is the path we see as the best path forward to getting to certainty and getting to the end. So, if you could imagine, that's a very long document with a lot of changes that has to be considered by each side.

And then, finally, there's a complexity introduced by the requirement that there is some community discussion on these issues. And I'm going to identify when that community discussion is occurring and can occur. But examples are validation of WHOIS information where changes in the validation process of WHOIS might add significant cost to a registration or a time to register. This is ICANN, so that discussion -- that change in policy has to be discussed in the community.

Also, the reveal of underlying data for proxy registrations, under what conditions that's published and to whom. We want to go forward with these changes with our eyes open so that the registrars at ICANN know but also registrants know and understand all the conditions associated with that.

So one item on the critical path to finishing on some of these is going to be public discussion.

So I just kind of -- did you want to say something, Volker?

VOLKER GREIMANN: Maybe just as an addendum. One further point is that we won't stop at the RAA discussions, of course. When these are done, then we will also continue discussions to find a way to bring the registrars that, for example, are still on a very old agreement, the 2001 agreement, I think it was, under some form of umbrella that they're also -- when the majority of the registrars signs up to the new agreement, that we have some uniformity and no outliers.

KURT PRITZ: And that's very good.

I kind of talked to this slide already, because I forgot it was here. But WHOIS validation, we're going to talk about that in about 10 minutes.

What does validation mean, identify the benefits, identify the costs. It's a public discussion.

So what are the next steps?

Well, in the current agreement, registrars have to renew their agreement if it's approved or based on a consensus. So, after the negotiations are finished, we will submit a whole agreement for public review. So there will be GNSO review of the agreement. There will be opportunity for public discussion.

The current agreement is fashioned in a way that the agreement is considered and approved by the GNSO. It's accompanied by a written report that documents the extent to which there's agreement and disagreement with these items, so that there's opportunity for robust public discussion and that discussion is memorialized. So, when the agreement is forwarded to the board, they will have the full record of that discussion.

And, as Volker just alluded to, when will this take effect? Registrars have 5-year agreements. Many registrars signed a new RAA in 2009. And this comes up again for renewal in 2014. So, upon renewal, the new agreement has to be adopted. Other registrars have signed at various times.

The registrars could voluntarily sign the new agreement early. We'll -- ICANN would work on an incentive package to incent registrars to enter into the new agreement.

Also, there's policy aspects to the new agreement. So, if the GNSO undertook it, they could undertake a policy discussion and make the amendments effective immediately, if they fall within what we call the so-called picket fence, those items that are policy.

So there's sort of an umbrella there about when the agreements will take effect and methods for accelerating that so we can get it done.

So, Volker, do you have some additional comments?

VOLKER GREIMANN: No. That summarizes it very well, I think. Like Kurt said earlier, the WHOIS validation issue is one of the issues that we've tried to tackle

within the negotiations. But we've realized very early on that this is a topic that does not affect only the two parties of the ICANN and the registrars but is, in fact, a topic that is -- has an effect on the entire community. And that is why we are not very -- not very well of making a determination on our own in a closed two-party negotiation but rather focused on a PDP or another policy building process for that.

And I think the WHOIS validation workshop that we're initiating together today is the first step in that process.

KURT PRITZ: Terrific.

So, with that, I get to leave and you get to talk about something interesting. So what is WHOIS validation? We use the term "WHOIS validation" quite loosely. And it's really related to a number of concepts. There's validation where we would assure the fields and WHOIS database is non-blank or contain data in the proper format. Authentication, which is data useful to, actually, reach each registrant. And then there's verification where data authentically corresponds to the true information.

So these are terms we've sort of adopted; but they make the discussion kind of confusing, I think. And I think, when we talk about WHOIS validation and when we respond to requests about WHOIS, what we really want is to make sure the WHOIS database is accurate. That's what this is about.

Excuse me.

And so how is this achieved? Because it will be a big change. WHOIS dates back to, essentially, the start of the Internet when it was used by college professors to find one another and question each other about why they were using certain servers or something like that. And the present uses were not foretold.

How do we make this fairly significant but important change right now?

Well, there's a range of models out there. There's registries and registrars and other entities that have techniques -- RIRs, that have techniques for validating information or authenticating information that it receives. Each has a different level of effectiveness. Each has a different cost.

As part of this discussion, meeting with law enforcement, discussing it with registrars, we put together sort of a range of tools, a range of authentication techniques that could be used that you could go look at. One, make sure -- you know, the top one. Make sure that this field isn't blank. And the second is make sure the phone number has the correct amount of digits for that geography and is a properly formatted country code.

Another level is write an e-mail and get a confirming e-mail back. And goes down and graduates all -- you know, down to, if you want to register a domain name, bring your driver's license, authenticate who you are. And we'll process the registration.

And different entities have adopted different tools for doing this. And one way to look at the different tools is that -- is at that link there.

So, once again, I talk about a slide before I get there. But what you'll see in that matrix is this sort of progression.

Are there blanks? Is it correctly formatted? Is the address deliverable? Gets more complicated. Is there patently false information that requires human intervention? Can you send and receive a confirming e-mail? Can you send a letter to the address and receive a registered mail receipt? Can you match the payment data to the registration data? Can you verify the phone number by either calling the registrant or having the registrant call you? Finally, is there a driver's license or a passport authentication? These are the types of models that can be used to validate WHOIS.

We should look at the purposes of validation, what our goals are in the end and adopt a technique that meets those goals in the most economical way for registrants, I think.

VOLKER GREIMANN: Yes. Our target here is not to overshoot in any way what is necessary to accomplish these goals. But we are very cognizant of the fact that each of these changes will affect registrations for registrants, for registrars, and also registries. All players, all parties in the registration process of domain names will be affected by any of these implications. And we are very aware of that. And also of who should play what role in this

process. So this is -- this is a very difficult topic for us to determine. And, therefore, we want to have a public discussion on that topic.

KURT PRITZ: So we think that -- that's the end. So we think that the panel we've put together is very cool. And they each have very specific and good experiences running these models. And I hope you enjoy this. There will be time for questions and answers after it.

I'm going to turn it over to the chair, who is Graham Chynoweth or better known as Gray. And he's going to introduce the panel. I'm going to thank him for his efforts in chairing this panel and moderating this discussion. And I want to thank in advance everybody seated at the table for participating and preparing. So thanks very much.

GRAY CHYNOWETH: Thank you, Kurt. Thanks, everyone, for coming. It was very exciting for us to be able to kind of lead the charge as registrars in organizing the panel because, you know, we're very cognizant of being a productive, effective member of the community. And we thought that one thing that would really help push this dialogue forward at the Costa Rica meeting was to be able to get people to talk not necessarily about what, because there's going to be a lot of -- that's a policy question -- but really about how. Because that really dictates a lot of what actually can be done, the solution set that is available. And we think that we've been able to pull together a fantastic panel who are going to be able to speak from a variety of different perspectives. We have people from the payments industry, from the DNS industry, registrars, and the security industry. And we think that across those we'll be able to learn a lot about what the options are for the DNS and the way that we do this to try to make a registrant experience, which is positive and efficient, but also produce results that increase the effectiveness of the WHOIS.

So with us today -- I'll just go down and briefly mention names, and then we can get into comments. The -- we have Eric Brown from Neustar, who is going to be speaking to the dot U.S. model. We have Benedict Addid -- I'm sorry, Addis -- from SOCA, who is going to be -- has experience as security researcher at HP but is now at SOCA; Xiaodong Lee, who has experience with -- well, he was with dot CN but is now an ICANN staffer, but speaking to that verification experience; Rod Rasmussen from Internet Identity to speak to the various experiences he's seen through his security work, especially in phishing; Rob Hall,

who is going to speak to his experience as a registrar and the other eCommerce businesses that he has on the Internet with verification and those contexts; John Curran, who is the NRO chair and will speak to ARIN's experience with it; Andrew Naumann, who will be joining us by phone. But we're really appreciative. This is very short notice for him to join the panel. But he's at Cyber Source and Visa. He'll be speaking to information verification from that perspective. And then Mike Stewart from CIRA, who will be speaking to the ccTLD experience in that part of the world.

So with that, we'll get into the speakers. I think we'll just go from left to right or from -- down from my left. And, John, thanks for joining us. And please take it from here. And just one last note on questions and answers. We're going to go through all the presentations, and then we'll have questions and answers at the end. So thank you very much.

JOHN CURRAN: Hopefully, slides will appear. I'm John Curran. I'm president and CEO of ARIN. I'm also the chairman of the NRO. The NRO is the organization where the RIRs work together on joint activities. You know us predominantly as the ASO within the ICANN structure. We rotate our duties among each of the executives. So this year I'm chair of the NRO. I'm going to be speaking today, very briefly, to give you a summary of what the regional Internet registries, the number registries, are doing in terms of WHOIS data validation.

We have an interesting situation, because we have the address records for all of the address blocks. All of the address blocks are maintained in a database called WHOIS, similar to what was used for DNS. And we have to keep those up to date.

And it's something that's been built over the years. And so, of course, we all run part of it. And there's an interesting challenge in the practices used to try to keep that current.

So let me move right ahead. Several factors influence the data accuracy of the WHOIS database for the RIRs. First, a number of resources have been registered since the beginning of the Internet. Every Internet block in use is a number resource issue to someone. So some of our records are old. And part of it is a refresh challenge more than a new issuance problem. That's one of the interesting aspects we need to explore on the panel.

Membership and service contract requirements. The RIRs predominantly serve ISPs, service providers, what's sometimes called local internet registries, LIRs. These are service providers who, in turn, issue address blocks to their customers. So we have multiple tiers. We're going to be talking predominantly about the practices that the RIRs use with their direct members, the ISPs and the service providers, not what the service providers are doing to keep WHOIS accurate for their customers. And that has interesting implications.

And then, finally, RIR business practices. Depending on the part of the globe you are, depending on the information that's available to validate organizations -- what records are online, what databases can you access -- you have different levels of validation.

We have five RIRs. I have to go through the practices of all five, so it's going to be pretty quick. But we do watch each other's practices, and we try to learn and adopt best practices from each other. AFRINIC, serving the African region, maintains accuracy through informal membership actions. When they talk to their members, they try to maintain and make sure they have accurate contact information. They review member data before billing cycles. They routinely check WHOIS contact information when members request additional number resources or new services. That's an important thing. ISPs come back seeking more addresses, and that's a great time to make sure that they've provided information about themselves but also about all the addresses they've allocated.

They have commitment through their RSA, their registration service agreement, to maintain their data accurate in the WHOIS. So ISPs contractually have an obligation to maintain that data. And staff also do a database consistency check annually where they look at fields in the database and try to find inconsistencies and update that. Now i'm going to talk about APNIC. You'll hear some of the same practices, maybe new ones. That will happen with each RIR as I bring them up.

APNIC maintains regular contact with its account holders in an annual renewal process and updates WHOIS accordingly. They note that they don't have a lot of changes, because a lot of ISPs maintain information in role accounts. It's not Joe Smith. It's XYZ ISP services, billing contact. XYZ ISP services, technical contact. So those don't change as people move in and out of organizations. Obligates the member to maintain

their own assignment information for their customers. They don't validate ISPs' customers ISPs are obligated to do that. Provide a public forum for reporting invalid details in which staff can follow up. While the records reflect address blocks that have been given to ISPs and to their customers, those assignments might be incorrect. And you can go online and say, "I see an address block here. I can't seem to talk to the party responsible. Can you investigate." And that's very common.

Perform annual WHOIS database cleanup process, again, a consistency check to help validate information. And then updates the WHOIS data whenever someone requests different resources.

ARIN, again, similar practices. We are obligate the resource holders by agreement to maintain accurate information. We provide a public forum for fraud reporting. We actually do a rolling annual point of contact validation with every WHOIS record in the database where we go out and say you must update your information or confirm it's current. And we tag records in the database that we can't validate. So there will be records that indicate the last date that ARIN was able to get a confirmation of current data.

LACNIC also reviews WHOIS data when resources are requested or updates accordingly. And I guess I want to highlight something. People come back asking for resources. That's a very frequent process. If you're an ISP and you're growing, you need more IPv4 resources or more IPv6 resources to connect more customers. And with IPv4 the size of the blocks you are assigned are relatively small so when you get your next block you have to show the assignment history of what you did with the last one. So we have a powerful motivation with IPv4 for organizations to keep their information up to date because if you can't show what you assign the last block to, you're not going to qualify to get the next address block.

LACNIC also updates data as a result of other efforts. Their outreach and communications with their members and they have a contractual obligation that their members, ISPs and service providers, maintain contractually accurate information. RIPE does a monthly review of about 50 records which results in about 500 or 600 annual audits. They will, when they get down to the end of the IPv4 address pool, the last /8 as they refer to it start doing a yearly self audit of the ILRs, the ISPs below them. They perform database queries to located and correct inconsistencies as well as database validation. They update legacy

WHOIS records as registrars update their addresses. Someone who has an address block from 10 or 15 years ago, when they come in, those are updated but a lot of these organizations are hard to find because the records come from the dawn of the Internet. They can make updates pursuant to their policies which is a policy called contractual requirement for provider independent resources. That says that when they issue policy resources to an organization, that organization is obligated to keep it up to date, and they check on that.

So we've got five different RIRs, very same practices but somewhat different. Each one is following the validation practices of its members, some 15,000, every service provider, hosting company, ISP is a member of one RIR or another. In each region they have set policies for what validation they think is appropriate for the region. While there's no consistent policy, there is a lot of practices that you can see are common along the RIR system. A global policy, because of the way the RIR systems works with global Policy Development, would need to be introduced into each region, would need to be adopted by their respective policy bodies and would come to ICANN for ratification as a global policy, if there -- if we were to have such for RIR WHOIS data. That's actually concludes my presentation. And I'm going to get back to the panel so you guys can hear about other people. Thank you.

[ Applause ]

JOHN CURRAN: Thanks, John. I think it is interesting to note about the geographic diversity that you had there, especially in the context of registrars who are obviously all over the world doing that kind of work.

I think the next speaker is Xiaodong. I think your slides are next. We'll see what pops up. Thank you, John. Yes. Xiaodong, I think you're next.

XIAODONG LEE: Okay. I thank you. Before my talk I need a clarification. You know, today's topics, I'm not on behalf of ICANN because now I'm the vice president for Asian Pacific of ICANN. So because last December I also resigned from the deputy director general of CNNIC dot CN, so I cannot represent dot CN and CNNIC today. So today I'm only on behalf of myself.

[ Laughter ]

But I believe that the ICANN community have a big interest on the dot CN WHOIS accuracy policy and experience. So today I'm here. I was invited by Kurt as an expert on this. So I always thought this topic in Kurt's presentation, you know, why we do the WHOIS accuracy. You know, there is a big argument.

When dot CN do this work, you know, we have many discussion about what's the user requirement, what's the government requirement, you know. For a registry maybe they want their money but for the government they want to do the amendment. It's a conflict. But as you know, there is a lot of domain name abuse in the -- talk about the (indiscernible) -- especially for dot CN. And, you know, in China they have a very strong requirement for the law enforcement, so how to manage the dot CN to spot the law enforcement is a very big issue. And in the slide I mentioned that there's regulation for the China Internet domain name management. You know, in this regulation admission the registrant must submit the true accurate and the complete registration information. It's a root published by the Ministry of Information Industry. You know, in the past year in this regulation and also the implement use of dot CN the individual registration was not permitted. That mean only that the company organization already used dot CN. But in the past years that so many people, they registered the dot CN as an individual because they can find the registrar, sign a contract with the registrar or find a temporary company to register the domain name for themselves. But after the WHOIS accuracy, you know, there's so many people, they cannot provide the certificate for the company information so it would be moved from the database. But now it was said that China will open the individual registries in the near future but I don't know the exact date, but maybe it's the next time. So what's the story for dot CN who is actually, you know -- I believe it's a true big challenge. Our mission, what is the WHOIS actually. You know, the user -- the registrar needs to post the address, phone, e-mail, the ID information, all the certificate information for their companies and so on, but the registry for the CN, the CNNIC need to check -- follow the rules defined by the Ministry of the Information Industry. They need to check if it is true, if the information is true, if it is accurate, if it is complete. You know, they also need to check the consistency between the registration information provided online and also the -- have a copy for the approval of materials. I think it is a very big challenge for dot CN. And how to validate that information. You know, that up to now even China itself there's no unique system online available to check the -- all

of the admissions. You need to check the user ID, ID information, you need to check the certificate of the company information, but how to check that online. That's a big challenge. You need two and a half years ago.

Now, how to protect the privacy is also a big challenge for the registry. You know, there's millions of user's information and millions of company information was submitted to dot CN but how to protect that. You know, last year there is a big -- you know, there is a very famous Web site CSDN and also now the social Web site culture, it changed dot CN. But there's a leakage for user information. There over 20 million user information was hacked, was hacked, yeah, and it was published for everyone. You can download all of the information. You know, even myself, I checked the day it was published. I found my information is even there. Even I forgot that. So, you know, there is so much user information is sent when the user is registering different websites, so that user information is sent. If this database was for public, that means all of the registry information in the Internet is published for public.

So the -- another challenge is how to deal with the legal -- legacy issues. You know, there are so many registries in the pastime. So I think we need to know what's the advantage and what's the disadvantage. You know, after the -- the WHOIS actually work for dot CN you cannot find so many DNSSEC abuse for dot CN. Maybe -- there's almost nothing for abuse for dot CN because every -- almost every dot CN domain name is registered by the real name. So many hackers or so many bad guys, they don't want to use dot CN domain name to provide the Web site or some kind of Internet service to do the bad things. So I still remember, I cannot remember the exact year, but dot CN fought many years, the second largest in the world. But now they cannot find that in the rank of domain name abuse.

Another advantage, the registry for dot CN can connect to the registrant directly. You know, in past years the registrar don't want to submit the registrant information to CNNIC. Even CNNIC run a thick registry. Yeah. So not all of the information you can get. So but after the WHOIS accuracy worked it can get all of the information because it's mandatory by CNNIC and mandatory by the government. You know, now there's so many people think that dot CN is much safer and it's much safety and much trustworthy domain name in the world because I think up to now there is 99% of the dot CN domain name is based on the real name and complete registration. And what's the disadvantage? You know, for the

registrar's number and also -- that means there is the income. Registrar's number means the income for dot CN. At the end of 2009 there was over 13 million, dot CN domain name registration, but in the last month the number is 3.3 million. You can see that's a big change.

Now the disadvantage is the cost increase. You know, you need to pay the facilities to do the WHOIS accuracy and you also need to hire so many people to do the WHOIS accuracy. In history the CNNIC hire more than 600 people to do that. I think it's a big cost in that year. And also in the year, you also need to pay money to outsource the validation service of money to some online service, yeah, to pay monies for some firm to do that because CN has only run dot CN domain names. They are not a law firm. They are not -- they don't have the database for user ID and don't have the database for company information. Another disadvantage is the marketing issues and the user experience. Even dot CN stop doing the WHOIS actually. They don't know how to do that. There's no standard for the WHOIS accuracy. What is WHOIS accuracy? How to do the validation? There is no stable regulations. So it give the user a very bad experience. They think ah, dot CN, we cannot use that.

It's very terrible. Yeah. There's no stable regulation for that. So there is so many arguments about dot CN domain names. Even the years before they were like that. And also, you know, in the marketing issues they think that they have a very bad impression for dot CN.

So I just summarize four questions for this. I think it's a -- from my point of view, I think it's a big concern about the WHOIS validation or WHOIS accuracy works. You know, you need to define the WHOIS accuracy clearly. You know, if you cannot define that, users don't know how to submit the information you wanted.

And the second issue is how to validate the information globally. You know, even as I mentioned even in China there's no unique online validation system. I believe that up to now there's no online validation system around the world. So if you want to do business around the world, how do you do that? You know, up to now there are many registration -- overseas registration for dot CN. CN cannot validate. You know, it cannot connect the user information validation system of other countries. It cannot use the online information system of other countries. So it's a problem.

And a third issue is how to protect the user privacy. You know, I think it's a very, very important. You know, when the user data transfer on the Internet, historic -- and maybe you need to do some backup, how to ensure you can protect the user information. I think it's a big issue. You will face a big lawsuit if you disclose the user information. And another issue is we need to discuss who lacks that. If the user lacks that. If the registry lacks that. If the government lacks that. I think if nothing happen, the user will complain that. But if you finish the work maybe some of you lack that. But I have no answer for the fourth question. I think we need to have further discussion or further thinking about that. So that's all the story. Yeah.

[ Applause ]

JOHN CURRAN: As one of the individuals kind of charged with potentially having to do some of this, I think it is fascinating to hear the concept or just how that rubber meets the road on hiring, you know, 600, 700 people to validate 13 million domain names. It's clear, you know, there's a lot of big implications for the type of things that we decide to do.

I think next on my list I had Eric Brown, and Xiaodong, if you could pass the -- have you got the clicker? All right. We'll see if your slides are up. Perfect. Thank you so much.

ERIC BROWN: Good afternoon, everybody. My name is Eric Brown. I'm a product manager at NeuStar and I'm responsible for all of our registry services. Today I'm going to talk a little bit about what we do in the dot US space which is one of the TLDs we manage today. We have a program that we call -- it's a formal name, we call the WHOIS accuracy program. It's evolved over the years. We've been running the registry now for about eight years, nine years and it's evolved over the years. We have a little bit of a different take on the way we deal with WHOIS accuracy. We focus primarily on post-registration validation or spot checks. We're not doing anything up front prior to the registration. We conduct random audits after registration and we focus a great deal on compliance and policy enforcement. And one other thing to note that in the dot US space we do not allow proxy registration data so we focus a lot on trying to identify and take down proxy registration data or at least get the registrar to clean up the data.

I'm sorry, did it go up? So some of the key components of the program. As I mentioned we do weekly random spot checks, and during those spot checks we're looking for a number of things. WHOIS accuracy is one of those things. We also have a nexus compliance program which is policy that's specific to dot US. We also perform weekly proxy WHOIS data searches which is a little bit different than random searches. We're actually looking for keywords in the registration data to find the proxy registrations. Registrars by and large are very compliant with this.

They're very aware of the dot US policy, so generally what we're looking for is third parties, resellers who might be not in compliance but by and large the registrars comply with this policy today. We also do two biannual manual reviews. We pull a very large random sample of data and we literally manually go through the data. Human beings, our customer support and other compliance personnel, we go through them, we look for data that is obviously inaccurate. Could be data that's missing, could be attempts to hide data. Sometimes it's simply incorrect data that may be the result of a faulty EPP command that comes in from the registrar.

We see that sometimes. For example, they leave off the country code and that changes the whole format of the phone number. We go through and we pull up and we create a report, we send it to every registrar. They're required to either correct the data or delete the registration or take it down.

We also do an annual review of every registrar's WHOIS implementation and that includes are they displaying the correct data, is their WHOIS responding, all the requirements that a registrar has in their WHOIS obligations. And then we also require, much like they do in the gTLD space, we require every registrar to send out an annual accuracy reminder e-mail to every registrant asking them to make sure their WHOIS is updated, to come in and correct any inaccuracies. And then also much like ICANN, we have created a WHOIS reporting tool. That tool is open to the public to come in and report cases of inaccurate WHOIS. It's also used to report nexus issues.

So a little bit on the random audits. I think that's a key part of our program. As I mentioned we do it both weekly and biannual. And part of our weekly random spot checks also incorporates any complaints we receive from a third party. We just add it to the list that we audit that week. And as I mentioned we're looking for missing data, inaccurate

data, mistakes. We will actually rate the mistake based on how severe we think the error is. If it's a -- a simple mistake by a registrar, that's rated lower than an obvious attempt to obscure the data or, you know, putting in 1111 in a phone number. We are not actually validating that data. You know, if we see an address that appears to be correct, has a valid ZIP Code, street, we're not actually validating that the registrant is at that address.

And then finally, at the end of the program, we notify each week, each twice a year we send a report to the registrar asking them to correct the data. There's a time clock that gets put into place and if they don't correct the data we actually take down the domain name. And that sums up the program.

[ Applause ]

JOHN CURRAN: Thanks, Eric. I think next, if you just want to pass -- do you want to click through? I'm not sure who's necessarily going to be next in the slides. Ah. There we go. Thanks, Mr. Stewart from dot CA. Thank you.

MIKE STEWART: Hi. My name is Mike Stewart and I'm from CIRA, the dot CA registry. We're rather unique I think among some of the other people at this table because not only are we a ccTLD but we're a ccTLD with eligible requirements. Without getting into all of the details, essentially our registrants have to have a connection to Canada and on a number of enumerated bases. So on the one hand you might think it's rather simple for us. We don't have some of the challenges the other people at this table have that they have to validate people all over the world. Excuse me. But at the end to have day we're facing many of the same challenges other people are. I was asked to keep the slides to one or two so I kept it very short. Of all the data I wanted to provide I just simply put in our -- the process we follow for validation, like dot US we don't do a lot of pre-registration validation. There is some of -- especially on the fields that are provided in the data that's provided.

But essentially we do the same kind of progress -- program of a spot audit. And by that we evaluate domains that we think are problematic and then verify them. As you can see here, they have a process by which we notify the registrant because like many ccTLDs we are a thick

registry and we have agreements with both the registrar and the registrant.

The registrant, like dot CN, is required to provide accurate and complete information and to keep it accurate and complete. So when we notice a problem through our spot audit process, we contact the registrant directly and there's this process for them to correct the information. Right now we're finding there's a number of low-hanging fruit in the sense it's fairly easy for us to spot issues in WHOIS data but obviously there may come a day hopefully where it's a little more challenging. But at the end of the day we decided to follow this approach rather than do a process by which it has a lot of in-line validation of the registration process because the concern we have is we're not aware of any simple easy solution to implement on a technical basis that will allow registrations to still be relatively easy and straightforward for our registrants and yet provide us with accurate WHOIS data in that process without making it massively complex. So we're very interested in seeing what some of the other people at this table and in the audience are doing to try to provide WHOIS accuracy as it's something we care about quite a bit. For us again, the real challenge is trying to find that balance providing accurate WHOIS data and yet making the registration process not horribly painful with people having to show up on our doorstep and provide ID for example.

The other issue we have is that while we can get people -- we can pretty accurately know that an address in Canada is accurate because most of our registrants actually are located -- have a Canadian address, that simply means the address is valid. And we can also do things that show that a particular person or a corporation exists, but particularly with people, you simply know, you know, a person's provided you with various ID, but what we struggle with is finding -- proving that that particular person lives at that particular address. And that's a real challenge we face as well.

At the end of the day, you know, our goal is to -- simply, you know, try to do the best we can do to get, you know, reasonably accurate data, but the -- that golden ring -- or that brass ring of perfect WHOIS data or a system of finding perfect WHOIS data during the registration process has still alluded us. And that concludes my presentation. Sorry.

[ Applause ]

JOHN CURRAN: Thanks for that. I think it definitely is interesting to see, your know, the similarities but I think also really at the end of the day, you know, how you're grappling with some of those unknowns. You can figure out if the address is valid but not necessarily whether it's connected to that individual person. You know, and these, I think, are the complexities when we start to get into these issues that are -- that really are good reason for us to have the panel. So thank you very much for that.

The next person we have, hopefully on the line, is Andrew Neumann from -- he's joining us from I think Seattle. Andrew, do we have you on the line?

ANDREW NAUMANN: Greetings, can you all hear me?

JOHN CURRAN: Yes, I think that -- I see lots of nods in the audience so you are well heard. Thank you for joining us. Andrew was on vacation last week and so got this request this morning to join us on the panel and has made time in his schedule to do so, so we really appreciate it. Your slides are up and I think if you just say "next slide," that will get you to the next slide down here. Thank you.

(Scribes receiving no audio)

ANDREW NAUMANN: What is the IP address that they are coming in on.

So it's a matter of collect being all this information, maybe augmenting it with third-party information.

And once we collect that information, then we go on to the business rules section. And this is where we configure rules saying, well, if they meet this criteria. If the shipping address doesn't match the billing address or it's a free e-mail domain or there's some level of risk associated with it. We want to ideally make an accept or reject decision. We want to disposition it one way or the other.

And ideally, we want to do this -- we want to make these systematic decisions -- we want to make sure that the majority of those transactions are evaluated systematically.

Obviously, some fall in this gray era and we are not able to make an accept or reject decision systematically so they fall into what we call our case management facility where we have a human reviewer looking at the record, doing some more deep -- deep analysis to figure out whether it is actually fraud or not.

And then that process typically should take less than 24 hours, and this will loop back into either an accept or reject disposition.

Ultimately you will see on your far right the fraud bucket, and what people do or primarily focus on is minimizing the amount of fraud that's associated with those orders or those transactions that you have accepted.

So if you click again.

So that 1% there, that represents the -- based on our recent survey, 1% of all revenues done by e-commerce merchants were fraudulent. And again, if you go back to that 2 to 5% range of costs.

So you can see that 20 to 15% of all costs are associated with fraud.

That, last year, represented north of $3 billion for e-commerce merchants. So it's a significant number. And again, the e-commerce merchants bear that liability and that cost, and certainly it's incumbent on them to try to reduce that.

But there are other costs that need to be weighed against just minimizing the fraud.

If you click again.

So you have this idea of, well, you've got orders that you have accepted, and some turned out to be fraudulent.

On the other side, there are orders that you have rejected and approximately it to 6% of all e-commerce merchants -- excuse me, 2 to 6% of all orders were actually rejected by merchants. And that, on the surface, seems like a very large number, and, you know, for sure there's probably, depending on the sophistication of the e-commerce merchant, there is a large percentage of those orders that may be legitimate.

So again, when you are looking at this problem, you always need to consider what we call the false positives or those legitimate customers who you inadvertently canceled, because there is a real cost. In some ways, that cost is more than the fraud cost that you have upset a customer and they will never use your product again or come to your Web site again.

And the other piece is, if you click again, is we talked about the case management piece. We work in an environment that needs to scale. E-commerce is growing at approximately 18% every year, and currently, anywhere from 9 to 35% of all transactions are now going to manual review, meaning that's probably far too many bodies being thrown onto a problem, and that will not scale effectively with e-commerce growth.

And what's maybe even more concerning is that 75% of those orders that do go to manual review and that are held up for, as we said, 24 hours are ultimately accepted.

So certainly that is, again, a poor customer experience and you need to make sure you minimize the amount of orders going to manual review and of those orders that do go to manual review, try to err on the side of not impacting the customer experience.

So where does this all go? And click one more time, please.

So this is really what e-commerce merchants are trying to resolve. And again, this should resonate with you folks.

How do I ensure that I'm making an accurate decision? How do I make sure that I'm doing it in a systematic way? And how do I do this as my business scales or as this whole environment scales?

So let's talk a little bit about the solution.

If you click again, please.

So data is really the life blood of our solution. And on the payment side, we have certain advantages that registrars may not necessarily have.

Specifically, we have more rich detail about what the customer is actually buying. As far as order detail data, we know the SKU associated with the purchase. Is it a plasma TV or is it maybe a benign toaster. Each of those have different risk profiles. So, really, the purchase characteristics are critical in making a risk evaluation.

The other thing we have on our side is we know a lot about the mechanism the customer is using to purchase it, purchase that item, as well as we have some interesting characteristics about the payer itself that they have offered.

As far as identity data, the payment piece of it, AVS. We're talking a lot about validation. There's something called AVS and CVN. AVS stands for address verification service. So every time you make an online transaction, you are going to provide your address along with your credit card number, so on the back end, the banks will return a code to the merchant saying, listen, yes, this address actually lines up and is associated with the billing address of the card holder.

Similarly, you are asked for your security code. We call this CVN, another form and widely adopted, at least in the U.S., and permissible form of validations. Again, you are validating that that instrument actually is in the possession of the card holder.

But we have also seen that these methodologies, as these crooks get smarter, and they are very sophisticated and very organized, the value of these indicators that are returned to us from the banks is diminishing.

The other piece we have is eyed identity data. Obviously you want your merchandise shipped to you, so we can get address validation, identity verification.

There is a -- in our field there is an adage that we don't want to create any friction in the pipeline, meaning we don't want to create anything, any impediment between the customer selecting his product and providing his payment details and checking out. So that's why we have always been very reluctant to put any validation tools in place.

We talked earlier about, you know, driver's licenses, passport information. Privacy concerns aside, that information for most consumers these days is considered intrusive and excessive.

So that means that the merchants need to rely on pieces of information that can be collected in the background. And I have highlighted two other pieces, and I touched on them earlier.

IPG location. So there's a lot of information that we can gather around a transaction based on the IP address that that transaction is coming in through. And we can resolve it to a time zone. We can resolve that IP address to a location.

So again, we're looking for disconnects between where the person says they are and where the actual IP address is located.

Similarly, we have -- we collect information about the device itself. Using browser and header information we're able to actually assign an actual identification or identifier to a particular device. S if we see that identifier again legitimate or an illegitimate order.

And also, we have the advantage of seeing history for a customer or a card going back in time. So we can say, well, this order is consistent with their previous purchase history or not.

And of course as a subsidiary of visa, not only do we see the card not present transactions, but e-commerce merchants, we can marry that with point-of-sale information, given us some real advantages.

Next, please.

So what I want to do here is give you -- you know, we talk about data, but I want to give you a concrete example of how we may use information and how the wealth of data is really important. And let me stress, it's not necessarily the data you collect but it's how you use that data.

And we have an example here of how we are able to detect normal versus abnormal behavior in order to identify fraud.

So if you click, it should start automatically.

So we have this customer, and you'll see that customer 1 has certain attributes, whether it is their e-mail address, whether it's their digital fingerprint or whether it's their payment instrument associated with different merchants and different purchasers.

Starting only at -- starting from the left and moving right, what we call that first order of correlation doesn't seem that strange. It could be a family member using the same card. It could be a family member using the same card across different e-mails.

In and of itself, that first level of correlation isn't that strange. But as you move to your right, what you will see is interrelationships between the different cards, the different e-mails, repetition that causes suspicion. And in this example, this would throw up lots of red flags for us.

You'll see multiple name changes, multiple credit cards being used. And by these correlations, we can identify whether it's fraudulent or not.

Next slide, please.

So it's also critical not only to be able to have this intelligence and this ability to see how things change and the data morphs over time, but also what's critical is to have a mechanism by which you can configure rules depending on the risk profile, meaning if I see this combination of attributes, I want to risk it -- I want to signal that it's risky is either send it to the reject bucket or have it side lined by case management.

So what we do at Cyber Source is not only hopefully provide the intelligence and the indicators, but an interface by which a risk analyst can go in and say it's suspicious or not suspicious.
Next page, please.

What you have here is just a screen shot of the case management interface. And what we're doing here is, as I said, there are some orders that you cannot disposition systematically. Of those you want to empower a human with as much information as possible in order to render the most accurate decision possible.

And here is an example of that case management screen and all sorts of links where you can go out to Google maps and see actually, well, is it a loading dock or is it someone's house?

There's a pop-up where we validate, you know, a phone number in this case. Additional observations. You can see how it's related to other orders. You can do other searches.

So this gives you a flavor that if and when you have to validate additional information or bring human resources to bear, be selective of when and where you do it.

So that should give you some feel of how we -- how we combat online e-commerce fraud.
So in conclusion, I'd say just be judicious about what information you collect. You really need to be sensitive to the customer experience.

Certainly be intelligent about how you use that data. Don't use it at face value. Look for -- There's never going to be one silver bullet. There's always going to be multi-factor solutions, meaning look at the data holistically and look at patterns within that data and don't think you are going to be able to solve this problem with a one rule fits all.

And also, make sure that you make the appropriate investments in your engineering infrastructure so that you can really focus on making systematic decisions as opposed to manual ones because this business is scaling.

Thank you.

[ Applause ]

GRAY CHYNOWETH: Thank you very much. There is wild applause, Andrew, so thank you very much for your time. We really appreciate it.

Next we have Rob Hall from Momentous.

Rob.

ROB HALL: I am going to stand, if I can.

I am Rob Hall. I am the CEO of Momentous. We own several domain registrars and other e-commerce businesses. I am also a member of the registrar negotiating team although I should preface this by saying my comments here do not represent the negotiating team or the stakeholder group, as you can imagine. We're in a competitive industry, and registrars, even among those on the negotiating team, often have

different views on different topics. So these are of mine and my company.

I am going to start off by saying something that might surprise you which is I believe any level of verification can be done. If you want us to verify identity, address, it all can be done.

That's not the important question. I believe the important question becomes what effect does doing it have on the market. And that's what I'm hoping to hear from a lot of different constituencies and stakeholder groups today as we go back into these negotiations to say what do you want. And as long as you understand what effects that has on the market and what effects it will have on registrants and domain holders and the ability to register a domain, then I'm okay with it.

I also don't think it's one size fits all, I want to keep in mind as I go through my presentation that registrars are the competitive level of ICANN, we are the competitive layer, if you will, that was created to be competitive. You don't need to tell us how to do this verification, you don't need to create a system that's one size fits all. I believe we will innovate at our level and figure out different ways and different business models to do the verification. What the community needs to decide on is what is the level of verification you want done, not necessarily the methods to do it.

One of the companies we own is called ZIP dot CA. For lack of a better term, ZIP dot CA is the NetFlix of Canada so we deliver over 40,000 DVDs a day by mail. It's a DVD rental system. As you can well imagine it's very important that we figure out who is the person we're delivering it to is at what address. So we are Canada Post. We are in the top 20 customers of Canada Post and are the only one of the top 20 growing and trying to find more ways to send mail. So we try to verify the address through the Canada Post database. So we have complete access to their full database of every address in Canada. It doesn't tell us who is at it. It just tells us the address exists.

The interesting problem we had right away was the format of it's difficult. There's rural routes, post office boxes, everything is a different field. We were trying to tell our customers you need to fill out these specific fields because it has to match the Canada Post database. That was problematic. We had a high failure rate of people he entering their address in way we be could verify it against the Canada Post database.

The other thing we found interesting, was Canada Post came and talked to us, was you could actually write a letter to me and put Rob Hall, Canada, K2E8B7, which is the postal code, and it will get to me because the postal code matters most in delivering mail in Canada. It will get it to the letter carrier and to the street, and he knows where Rob Hall is typically on that street. So trying to match addresses, people would commit fraud with us saying hey, I'm at this same address and they just teak a little bit of that address. It's the same building but they're getting second two accounts or free accounts at the same address which we prohibit. We said how can we verify this person's address, and we came across two credit checking, Trans Union and Equifax are the two largest in the Canada. I believe they're the two largest in the United States. And we started verifying every single customer with them and saying does this person actually live at that address? We found that not to be very effective as well. Most people gave us a proper address. The ones that didn't were so good about it that Equifax and Trans Union were not able to screen them out for fraud.

And then we started sending our first shipment by traceable courier, because we are actually sending a physical good as opposed to all my other businesses which is a virtual good of a domain name and delivering it instantly. This had value that we were actually shipping.

I can tem you that we have stopped all three of these practices now, because we found them not to be very effective on the people who didn't want to give us the proper information.

So customers that said, yes, I want to give you the information, I want to get my DVD, always passed. The fraudsters figured out ways around all three of these. So we decided there was no appreciable effect any of these services had on people actually giving us proper information. We had to eat the risk. And as a business not regulated, we chose not to continue spending the expense on Trans Union, Equifax and tried putting our customers fit being through that address database of Canada Post. And interestingly enough, our corporate address of Momentous is wrong in the Canada Post database. It causes us grief you cannot look us up in the database. We have to give a wrong address of where we are in order to get the process approved through the automatic verification, which is crazy.

The other big company we run is Pool.com. And the interesting experience there is early on our customers demanded we separate account data from WHOIS data. Very early we learned they were putting data into our account data, like domain administrator. We said no, no, we want your name in here. This is how we are billing you. This is who you are. And they said we don't want that public. We want a placeholder, if you will.

So Pool separated out account data from WHOIS data. I can tell you much more accurate data is provided on the account data. People are choosing to not provide relevant or accurate or personal data, if you will, to the level they do on our account level in the WHOIS database.
So as soon as we separated the two issues, the data became radically different. Customers don't want to put their real WHOIS in, mainly because it's public. They tend to want to put something that refers to a position or a role, as the gentleman from ARIN suggested, as opposed to putting their actual name and address in. We heard a gentleman talk about Verified by Visa? There's no address verification service offered by Visa in Canada. That's an American product, so we are unable to verify an address on Visa, when we process a Visa. We're also unable to verify the name on the card. It's simply card, expiry date, and the CV number on the back.

What we started doing recently was using a product by Visa called Verified by Visa, and it verifies that the person owns the card that is actually giving it to us, but it gives us no information about what the identity of that person is. It just assures us more prompt payment.

NameScout is one of our registrars. It too allows separate WHOIS and account data, and customers are demanding control of what they put in the public space. So we found by and large, customers were happy to give us more accurate data on the accounting level than they were on "we are going to publish this data on a public database."

I am going to talk about field level verification and all the different types of verification to make sure we are all on the same page. Field level verification is what others have spoken earlier. It has data and where possible it is in the right data format. You can't put a four-number phone number for Canada. That's an illegal format.

Cross field validation gets harder. That's where you are saying the postal code matches the city or the country even.

It's important to note a lot of people think we can do telephone number to area. In other words, is the telephone number in Ottawa. I can tell you a lot of people are using Google voice now or cell phones where it's impossible to tell what area code the number is in. It would be hard to narrow it even to Canada and the U.S. but you could certainly narrow it to the plus one country code.

And then something that I call verifying the contactability. And I know contactability is not a word as was pointed out to me earlier but a it's too late, of e-mail, phone and postal address. What do we mean by this? I think a lot of services say who are you, what's your e-mail address, and we are going to send you a key to it that you click on and say, yes, I'm reachable at that address. That does nothing to say who I am and I'm Rob Hall and what my identity is. It just says I am reachable at that e-mail address.

The interesting experience I had two weeks ago is I signed up for Amazon's cloud services. And during the process of signing up on the account they said we need to verify your phone number. I thought this will be interesting and timely. And they asked me to type my phone number in and they said when you get the call from us, type in this four digit number on your phone's keypad. I pick it up; it's Amazon's automated system calling. I type in the four digit number, and my computer screen changes to "Thank you for doing that. We now know you are reachable at that address." They still have no idea I am Rob Hall, but they have done one easy step to say, yes, I am reachable at that phone number.

And the last one is the hardest, of course, which is the postal address.

[ Speaking too quickly ]

We're not talking about is it a valid postal address here. It's are you reachable at it. And in theory, you could do something similar of sending a key to it. Identity verification is much harder. So proving I am Rob Hall is the hardest thing a registrar would ever need to do and we need to think hard before we say yes, that's what we want. Is it really contactability we want? Is it really identity verification that we want? But what check at what level we do is what we need to decide through this process of what we should be doing for verification.

The other question that comes up a lot in our negotiation is when do you do it. Do you do it at registration time or 30 days after registration time? Do you do it if they change or update the information? That seems logical. I updated my e-mail. Do you verify? Do you do it when you get a complaint from someone saying hey, this information is wrong. Do we do it with the annual WHOIS reminder? If that bounces or is wrong, maybe we should check other things.

But we need to take a step back and say what's the purpose of it. If the purpose is to see that that person is contactable at that information, that's a different standard than saying the identity is Rob Hall.

What are some of the dangers? I will wrap up with that.

We have to be very careful the level of verification does not cause what I call nationalization and the ghetto effect. If you tell me you want me to verify every single person's identification in person before they can register a domain name, I say I can do that. I will go out and do a deal with Canada Post or bank of Canada and say you have to show up to their offices and prove their identity.

But it creates what I call the national registration of registrars. I'm not going do that in very many countries. I might choose to do it in the U.S. But Senegal, I'm probably not going to open an office there or in -- a lot of the regions of the world will be unserved. So we have to be very careful that whatever we do put into place doesn't just serve those with highly automated databases and systems such as Canada and the U.S. where verification might be easier than it is in third world countries.

I think the other thing we have to be careful about is that stringent requirements can actually lead to bad data. I'm sad I'm saying this in front of the chairman of ARIN. But we have an IP address block at ARIN that has had old data on it for about four years. And the only way to change that, I found out recently, is for the director of the corporation -- and that's got to be me -- signing an affidavit in front of a notary to change the contact person on it. This hasn't been done because it's just such a pain in the ass. We'll get around to it at some point, I'm sure.

But It was interesting to me that the reality was the thing works. I don't need to make changes to it. Why am I going to all this trouble to simply correct an address because someone left my employ four years ago and the data of the contact is now stale. We have to be careful to not put

on requirements that lead and cause more bad data once it becomes stale. We want to make it easy for the person to change.

I want to be careful not to take a step backwards to old technologies. We're the Internet. Now we're talking about doing things over postal services and sending out notices in regular mail. It seems almost like a step backwards to me. I think we can do it in extreme circumstances, if warranted. I'm not sure we want it to be the norm to register a domain on what the new frontier of the Internet is as compared to the old technology on the old frontier. The other concern I have is we seem to be creating a data set called WHOIS data that is different than all other data. I believe, when we speak of WHOIS, we often mean many different things. We talk about privacy in WHOIS. We talk about verification and accuracy and SLA agreements. And I think we do ourselves a disservice by rolling all of these into one big debate. I'm not sure we'll ever get to the end of it. But the one thing I do know for sure is customers seem to be happy to provide more accurate data if it's not being published publicly.

And I don't know how to solve it. I know this has been a huge debate for years at ICANN. But I heard yesterday an interesting point in the GNSO, which was they've identified that the customers of this data seem to be law enforcement and what I'll call private law enforcement, which tends to be the intellectual property groups trying to enforce their legal rights through civil means. So I'll call it all law enforcement, whether it be criminal or civil.

But they seem to be the largest users of the data. So I have no idea if it's possible to find a way to give it to them separate from making it public. But the big fear from our clients seems to be we don't want to make this public. If you're going to make it to be public, we'll give you something that's rather useless. I don't know how to combat that, other than to change the perception of the people giving me information such that they want to give me the information and they're happy to give it to me and I'm protecting it in the way they want.

That's the end of my presentation. I'm happy to take questions later. But I'm really looking forward to hearing from different parts of the community, what should we be doing? Because I think that's the crux of what we're trying to get to here. I think registrars have come up with many inventive systems how to do it. We just need to decide what should be done. Thank you.

[Applause]

GRAY CHYNOWETH: Thank you very much, Rob. Next -- you want to click, and we'll see what slide comes up next. I'm not totally sure. Benedict.

BENEDICT ADDIS: Almost got my name right.

GRAY CHYNOWETH: Thank you very much, Mr. Addis. You can see how bad information sometimes makes it even into the best of circumstances.

Thank you very much. And take it away.

BENEDICT ADDIS: Hello. My name is Benedict Addis. And I currently work for U.K. law enforcement. That's the Serious Organized Crime Agency. I'm here, and I used to be a techie. I used to work as an engineer at Hewlett Packard Labs in Bristol. And before that I worked for an e-Commerce company. I actually ran an e-Commerce company.

So, if you're here as a registrar -- and I can see a few, and there's one beside me -- I want to say that I understand some of the difficulties you face and some of the issues around your business models.

So a little bit of background. I'm here as part of a group of law enforcement from the U.S., from Canada, from the U.K., from New Zealand, from Australia. And we've also got support from INTERPOL, which is the international policing organization and from other organizations.

So about a year ago, this group presented 12 recommendations made by international law enforcement. I'm looking at Bobby Flaim, who has been leading on this work.

And so, in the ICANN structure, these law enforcement recommendations, this packet of 12 recommendations are being passed up through the GAC and then to the board. I think so far, I think 10 of these are fairly uncontentious, that we've more or less reached agreement that 10 of these recommendations, which have to do with kind of common sense stuff, like thou shalt have a contract number on

our Web site; as a registrar, thou shalt have an abuse contact on your Web site. These recommendations are open and public documents. So you can read that on ICANN's Web site. There's nothing -- there's no kind of closed doors negotiating going on here.

Two of these requirements have met a lot of resistance, a lot of pushback. And I think that's as much our fault as anyone else's. Because I think we haven't been very clear about those recommendations. So one of the things I'm here to do is clarify one of those recommendations.

So, so far, Rob and Andrew have both talked about private data collection. So just like any other company -- and in the U.K. we often think about mobile phone companies as being particularly interesting to law enforcement. They hold a lot of information that we need to get in order to detect and prevent crime.

Similarly, registrars hold a lot of transaction information that they gather as part of an online sale on their customers. So you've got an I.P. address. You might have some HTTP header information, and so on and so forth. So we refer to that as private information. I'm not going to talk about that collection. What I'm going to talk about instead is the validation of the WHOIS, so the public information that we'd like to see improved.

So I guess the big question is why does law enforcement care about WHOIS? You know, we sat on the GNSO yesterday. And there's been a huge amount of disagreement about this.

I think Judith Vazquez called WHOIS a museum piece.

And I think there's an obvious reason that my colleagues will nod their heads about, which is that having WHOIS, even if it's not entirely accurate, is a start. Okay?

It's what we in law enforcement call a lead. It's a starting point, right? So, even if the e-mail address is incorrect -- whatever we mean by incorrectness. We can philosophize about what it means to be me and what it means to have that linked to an e-mail address. But we might have seen that e-mail address used in connection with another criminal activity, just as we might see -- we might know that a gun has been used in two crimes. We don't know who fired that gun, but we've linked it

together. So that's useful information. And, ultimately, that leads to attribution that we might be able to find the person that did something bad on the Internet.

The second and more subtle point about WHOIS is that -- and this is very much -- this is a subject very close to me, because I work in an area called "prevention and disruption." And that means pushing the -- gosh, that's popping terribly -- that means pushing the bad stuff, sort of normalizing -- being a good Internet citizen, so normalizing the idea that the WHOIS, such as it is, be correct and accurate and pushing the bad stuff to a corner. So we denormalize criminality. So that's the more subtle point. I think we achieve that by raising the bar a little bit.

Often registrars find it difficult to understand why we would want to make it a little bit harder for the bad guys. They say, well, the bad guys will just change their M.O., as we call it, the modus operandi. So why are you asking for this? It's trivial to circumvent. I think we say, well, you start to put these measures in place. And, frankly, at the moment, some registrars will even accept a registration that has blank fields. So all we're asking is to make it a little bit harder, to make it a little bit less trivial, and to reduce new entrants to the field of cybercrime, which at the moment is quite easy to get into.

So I think I've got my -- I've only got one slide to talk around. I took our requests seriously. And this is a mechanism that we've come up with to validate the WHOIS.

It's a bit complicated. It looks a bit scary at first. So I'm going to talk you through it.

The first thing to understand about this is it's a scoring system. Okay? So every box is a score, a point, if you will. And what I've done here is formalize a lot of the discussion that we've heard from Andrew and that we've heard from Rob about how and where we can check.

So the first line -- and, as you've seen, the arrow shows up on the right-hand side. So at the top it starts easy. And that's easy for the registrars. Really easy to check. But also easy to complete for customers. So the idea is we start with some points that are -- that are not going to add burden and add costs to the registrar business model.

So you can get four points just for checking that there's an e-mail address, there's a phone number, there's a postal address, and there's a name.

Now, this sounds incredibly trivial. But we regularly in law enforcement see cases where this information is not complete. So that's four points right there. Four easy points. For the techies in the audience, that's achievable with some very simple JavaScript.

Second line -- I'm getting a hurry up sign from Bertrand.

The second line -- and, again, these are international standards. So they're probably the most unappealing to look at. But they, basically, say is the e-mail address formatted correctly? Does the phone number match international standards? Does the address match international standards? That's the International Postal Union standard. I can't think of anything for a name. If anybody has any clever ideas about this, let me know afterwards.

So, again, this is all something that could be done in the browser or on the server free once you've implemented it. There's no cost to that. Does the e-mail address look right? When we first developed this graph, this was called "Does It Look Right?"

On the theme of no cost, moving down to the third line, the yellow line, consistency. Now, this is the cross field validation that Rob has talked about. Now, unlike with the private data, this is public WHOIS data. So we don't have the luxury of checking against all sorts of other records. We've just got to take this record, this WHOIS, on its own merits. So we can ask the payment company whether that's -- whether we're providing our own payment services or if you're using an external payment service provider or merchant service provider. You may be using Paypal or World Pay. You can say does the e-mail address, the Paypal address you paid with, match the e-mail address declared? You can say does the international direct dialing code, the IDD, match the country of registration?

Does that country match the bank identification number, which is the first six digits of your credit card? I'll actually identify a bank with the first six numbers on your credit card. And does the name match the account holder on that payment account?

Now, we appreciate -- and I have a background in e-Commerce, so I know that sometimes you can't always get this information from your PSPs and from MSPs. Sometimes it's for data protection requirements. Sometimes it's for business reasons.

So the -- this model has been designed to be flexible in order that, if you can't match these requirements or if your customers contact you in other ways or if they pay in different ways, then there are other ways to score points to reach a certain threshold.

Line 4 is something we talk about all the time, and it's pretty straightforward. But it's the first time that costs can be occurred per check. Check an e-mail address exists. You might want to check that the DNS is resolving. You check. The check the second part after that. You might check that there's an SMTP service that actually responds to that e-mail address. You're not sending an e-mail yet. You're just checking that that e-mail address is on the Internet, in some sense. The phone you might check. We've heard a lot about how to check phone numbers and how to validate those.

Again, the address we can check against the card address. And, for the first time, it's possible to check a name against a telephone directory, against third party servers, against even Facebook. There are going to be some business models that are going to integrate with Facebook, for example, and that will allow you to register your domain through Facebook. So the point and intent of this framework is to be as flexible as possible to enable innovation and innovative business models.

The final line is the one that's -- I guess, attracts the most controversy. Because it involves a serious cost. And sometimes it has implications on privacy, as we see it. E-mail validation is pretty non-contentious. You send a link in an e-mail, and you get one back. A telephone number, as we heard, make an automated call. And, as the Spanish registrar interdomain found, when they were trying to fight Conficker and Conficker domain registrations that we used to control this enormous botnet Conficker, they asked all of their customers to provide a mobile telephone number and to reply by SMS, to enter a code that they'd received by SMS. So there is precedent for these things, but I understand -- we understand that there is a cost to do these.

Again, we've got the old Nominet system under address. We can validate an address by sending a letter with a code on it. When I paid

80 pounds for my dot code U.K. back in the late '90s, I was sent a letter. And it had a code on it, and I had to scratch that off and enter it on a Web site.

So we don't -- I think the point to understand is we're not proposing something that stringent as a request for every registration. That would be ridiculous. What we're saying is that, if your business model is such that you cannot make any of these other checks, if you're in a developing country where there are no good ways to do some of the other checks, that it might be feasible, instead, for you to rely on a postal service. So this is about enabling access to the domain name system for developing countries and for alternative business models. It's not about mandating these requirements.

So law enforcement and the GAC is saying to the registrars tell us how you want to validate, tell us the costs involved, and let us know where the threshold should lie.

Now, I'm just going to make one comment about this, which is to say that, if you have a scoring system -- and my proposal it is this should be a public score, published alongside the WHOIS information -- you can then put all sorts of measures in place about border case, about edge cases.

So, if you've got a registration that you're not really sure about, instead of refusing it and refusing that person's money, you can say, "Okay. We'll take your money, and we'll take your registration. But you have to wait for 48 hours, or you might have to provide some more documentation." So there are -- for the first time there is a graduated response possible and being proposed to registrations.

I think we'll leave the slide on the screen, because I imagine there's going to be some discussion about this. I can see from your faces.

So I thank you very much for your attention. And, please, any questions would be welcome.

[Applause]

GRAY CHYNOWETH: Thank you very much. I think we're actually going to -- the reward of the last word goes to Rod, who I think will finish this off. Thank you very much.

ROD RASMUSSEN: Okay. I will be brief, which I know most of you think might be unusual.

My name is Rod Rasmussen. I run an security company called Internet Identity. We have experience on this from both sides, trying to track down either bad guys that have registered things or good guys who have had their sites broken into and we're trying to find them. And WHOIS is one of the ways we do that. We also work with lots of banks and e-commerce companies and, actually, provide reputation data that they use in order for scoring transactions and things like that. We deal with these kinds of things in various industry groups we're in. The last three, in particular, presentations really hit on a lot of the themes I wanted to talk about, which is this, really, risk management issue overall.

We need to treat it that way. This is not a one size fits all problem. And there's not a single solution. But you have to align your goals for what you're trying to do with what kind of context you're in. In an e-commerce situation you may be doing something very simple where you're assigning, say, a free e-mail account to somebody. Or you may be selling them a plasma TV, which will be shipped to them. The risk is borne differently in various situations. And I think that's an important thing to remember here in the case of domain registrations. We have a case of asymmetric risks in that, to the domain registrar, you may have the risk of a returned credit card or some sort of payment that does not go through as kind of the outstanding risk factor to the organization.

However, the use of a domain name can have a very wide impact on many other third parties. And that does not directly affect you.

And so I think the appropriate models to be looking at are more where you have an asymmetric risk. I think a good one to look at is money laundering and the banking industry. Banks make a lot of money by people moving lots of transactions through those banks. And, as a result, you have a situation where they do not bear a whole lot risk if a single transaction is stopped. Or they lose a little bit of money if it's a stream of millions of dollars have gone through a bank over time.

Hence, you end up with anti-money laundering legislation and very, I think, kind of very burdensome regulation in that industry where most large transactions have to have a report filed on them. I don't think we want to end up in that kind of a situation in this industry. And I think we can very well control that. But that is an area where you have asymmetric risk that is not a bad one to look at for where you have to deal with these kinds of issues.

And a key thing here, too, is that not all transactions are the same. Not all transactions have to go through in a timely manner. We were just discussing that. You do not have to provide service to everybody who asks you to do service or who you provide service for. Not all transactions are equal.

This was already covered in greater depth and detail. There are lots of ways of dealing with things of scale at various points of the process, whether it's from easily accessible formats of what fields should look like to services that can -- that you can use to get information about people, and are they really at that location?

A lot of the people search services out there are very robust. And they compete with each other in order to provide services in that area.

I think one thing we didn't talk about as much is reputation systems. There are many -- and they are growing out there -- where you can actually get information about various Internet infrastructure, whether it's an IP address, name servers, e-mail addresses that have been used in context in other places. More and more people are providing that kind of data back to people who are -- and, typically, you have to pay for it. But not always. There's free services out there as well. (Indiscernible) and Spamhaus, for example, offer that kind of information out in many contexts, so that you can actually take a look at things. Geo location was already mentioned as a service. It's a very good one for being able to easily track things and score things.

The idea here isn't to put every single transaction through some sort of process where it has to be highly scrutinized in each one. In fact, it's rather the opposite. You want to routinize the things that are normal. If you have an existing customer ordering domains on a regular basis and you do not have problems with that customer, you probably do not need to have that same level of scrutiny on that kind of information that's being provided as for a new customer coming in. That's the same

for an e-commerce situation as well. You do not -- if you have things that come in that easily pass checks, that's great. You pass it along. And I think it was already mentioned that you can pass those kinds of things along quickly, and then you save the more riskier transactions for either a higher level of scrutiny where you might actually have some sort of paid service that you tie into. And then, if it fails in that regard, then you may have a manual review process. But, again, it's not putting everything through the same process all the time and being able to look at it from a risk management perspective.

In the end, there's various ways of dealing with this, whether you have the manual review or some sort of third party looking at it. There's also escrow services that say okay. We'll allow you to take this transaction, but we'll put it in some sort of sort of state where we can confirm that it is being handled properly. And then, of course, you always have the option of not having a transaction at all, if you think there's too high a risk of what you're trying to do.

And those are all the slides I had. So I actually think I kept it short.

GRAY CHYNOWETH: Thank you very much. The clear point from this panel is there are, certainly, lots of ways that information verification happens. And there's a lot of implications for any of the choices that get made and if they get made about how this will happen in the context of the WHOIS we all know and love.

So I guess we have a few more minutes here. This goes for another six minutes, this session. And I'd invite folks to come up to the -- audience -- I have -- given it's so short, I'm going to put in 30 seconds, because I want to try to get as many people as possible. So, with that said, go. And I'm going to try to be very hard about 30 seconds.

I'm tracking now.

>> No, you can't -- Kurt wants the time.

GRAY CHYNOWETH: Kurt wants the time. It it's not off your time.

KURT PRITZ: So the good news is the presentations were fantastic. And so thank you all. The bad news is we spoke too much. And we're, essentially, out of time. So we can take a few questions. So we have some options. We could make this part of the public comment session that's already scheduled. Or, if the panel -- some or all of the panelists come back, we could schedule another session for Thursday just to -- just to answer questions. So I'm just concerned that we cannot run over. We have people calling in from all over the world for the next session.

So we can take a couple questions. And I recommend we schedule another session, a follow-up session, to answer questions on Thursday. So, with that, we'll take a few minutes to take some questions. Everybody gets 30 seconds, and then we'll cut off.

>> Kurt, just to give you information, quick poll here, only one of us isn't available Thursday. So we could do that. Is not. So we could do that.

KATHY KLEIMAN: Kathy Kleiman with the WHOIS team. I'm not here to ask a question but to give a commercial. If you really want to continue the discussion on things like reducing blank fields in the WHOIS, standard of contactibility versus absolute verification of all data, low hanging fruit -- you'll hear the very same terms right here in this ballroom at 4:30 as the WHOIS review team presents its final report and its recommendations. Thank you very much for your presentation.

>> Thanks, gents.

JAMES BLADEL: Hi. James Bladel from Go Daddy, also a member of the WHOIS review team and echoing what Kathy said. I just wanted to make a few quick statements. Thank you, Benedict, for that chart with the 5Cs. I've been present for every registrar law enforcement discussion since Seoul. And that is the most helpful five minutes I've seen on this whole topic in two years. So I wanted to get that out there.

Secondly, Rob makes an important point about ghettoization, increased risk as they pull back out of --

(Scribes receiving double audio feed.)

This cannot be a question that registrars and staff go off in a room and solve -- open multistakeholder PDPs. There's too many folks here who have questions. We have too much at stake in this issue.

ELLIOT NOSS: Elliot Noss, Tucows. I think that, sadly, we are all missing the opportunity and the point to get at the bottom of this question. You all did a great job of proscribing solutions. No one is talking about the problem. We're presuming that there's a problem. I was not once a geek. My wife was a criminal lawyer. Therefore, I have experience there. There was a tens of billions of dollars theft problem throughout the developed world. We don't strip search everybody walking out of every store. It would be super helpful, if we worked together on solving the problem. And the role that especially law enforcement can play is in defining and outlining the problem. We work greatly together on problems that aren't proscribed like phishing and spam. So please focus on the problems, not the solutions. Thank you.

>> I'm from Egypt. Thank you for the excellent presentations. We haven't heard anything about the WHOIS and multilingualism. I think it is becoming vital to start to consider this, specifically from a market point of view, from law enforcement point of view issues as well as -- and today we are including ccTLDs and IDNs fast track very successfully. This morning we have been following a very interesting presentation about gTLD. I understand it allows as well multilingual gTLDs in the future, so that there will be a need definitely for WHOIS in a multilingual form.

So maybe, Dr. Lee, you can comment on is there any work in this direction about the IETF? It will be vital for multilingual in the future and law enforcement agencies. Thank you very much.

GRAY CHYNOWETH: Thank you. We have time for two more.

STUART LAWLEY: Stu Lawley from dot xxx ICM registry. I wanted to let you know what we're doing and how much it's cost, because we've recently done this stuff. Very interested in Benedict's 5Cs. Hopefully, we score at least 3 on your Cs. So I'll let you know what we do and how much it's cost us to do it, just to give you a flavor. So we do an e-mail out verification. We don't stop the purchase process. We let people buy. And the name

doesn't go into the zone until they're verified. So there's no cost abandonment. We work with 192.com who amalgamate all this data. We built our own customer relations management CRN software, which cost about $100,000 in development costs. 192 and Dun & Bradstreet are all iterated. And, depending on which country people are in and whether we're looking them up as business or personal -- U.K., we can check the credit reference agencies, the director's list, the list of deceased people, electoral roll, forward ID, telephone number, and KYC. We can do things in U.K., Canada, Germany, USA, and Sweden. Other countries we can't do so much. It's a based on the credit. We're on the credit system. Each credit costs us 30 cents. So, as a minimum, it costs us $1.80. As a maximum, it's 7 bucks 20. On average it's $6 per verification. On average on our user base, each of our registrants is buying three names. So it's working out at $2 per name. (Scribes receiving double audio feed.) We also do a telephone out via box. So you're in front of your PC, you get a realtime phone call in seven different languages with a 4 digit PIN number you type into the screen. So e-mail and phone number is an absolute must pass. We also do geo targeting. IDD phone number. And we have a point scoring system ourselves. We may let people go ahead. And, depending on how risky they are, there's a must pass level to get resolved. But then we have three customer service people full time doing this. And they have their target list of people to be reaching out and, if need be, get copies of photo IDs. We also have in the adult TLD, a lockout system for people who enter date of birth under 18. They're locked out, and they can't reapply. They have to do manually and photo ID --

(Scribes receiving double audio feed.)

GRAY CHYNOWETH: Thank you, Stuart. So last comment. Sorry, guys.

MICHAEL PEDDEMORS: Thanks very much.

I'm Michael Peddemors, president and CEO of Linux Magic. We do a lot of work in technologies for North America now into the emerging markets. One of the things I want to point out is we're trying to look at all kinds of complex ways of doing WHOIS and everything else while we have a very traditional service that, frankly, isn't being effectively done right now. You've got people with class 16s and RIRs who don't have functional WHOIS services that just aren't responding. You've got

hosting providers who aren't posting the most rudimentary information like the customer's name. We know there's a lot of privacy concerns, but I work a lot on creating these reputation services such as spam rats. And it's very important to be able to do some highly scalable, very quick, very simple checks. And, similar to the guy from SOCA was mentioning, just simply seeing that one name shows up, 15 different hosting providers with the same pattern would ask that ICANN be more strict with its own people right now and maintain what some people call is a dinosaur is an extremely effective tool. We just want to simply have an accurate name, and that's it.

GRAY CHYNOWETH: Thank you very much. Next -- I'm going to try to get closer to 30 seconds, please.

(Scribes receiving double audio feed.)

GARTH BRUEN: I'll do my best. Garth Bruen from NARALO at-large. I think it's interesting that NeuStar and Momentous are on this panel, since a Momentous company offers privacy services within dot WHOIS in violation of WHOIS policy.

My question is actually about the amendments as they're written. There's nothing within the list that actually gives ICANN the authority to enforce against a registrar who does not delete a domain with invalid WHOIS. So what is the point of doing this validation exercise? Thank you.

(Scribes receiving double audio feed.)

WENDY SELTZER: Wendy Seltzer with the non-commercial stakeholder group. Series of questions: What problem are you trying to solve? How does ICANN's problem compare with those of credit card companies with the country of China, et cetera? False positives. Can we afford to get human rights advocates knocked offline or worse, because they're identified through their WHOIS or denied access to register a domain name? How does identification scale to the global Internet, particularly to developing countries? What kinds of barriers to entry to new Internet businesses are we proposing to set up here if we impose verification requirements

on those in countries that are harder to reach and people who are newer to the Internet? Thank you.

GRAY CHYNOWETH: Thank you very much.

[Applause]

MIKE O'CONNOR: I get last word. This is Mikey O'Connor. I don't know what I am. I'm a member of a bunch of stuff.

Just a few observations. I love all the gradation discussion and all the shades of gray stuff. This is clearly a nuanced conversation. And I am very cheered by the obvious trust building and collaboration that's starting to emerge. It was lovely to have Rob and Benedict right beside each other. And -- take that picture. Somebody take that picture. That was very cool. When I go through panels, I love to say "yeah, like he said." And then "Oh, yeah, like he said" and have the two of you kind of on the opposite side of the table. So big plus 1 for that.

Because it's gray, I want to chime in on the public transparent process. I think that's a very good step.

But I also want to chime in on the don't proscribe solutions. I don't think policy does that very well. So, when the policy gets made, we should try and make high points that are easy to hit in a variety of ways.

And then, finally, just one sort of last new point, which is there are a lot of people in the peanut gallery that are throwing a lot of grenades right now. If we can tone down the external rhetoric and the sort of noise that's coming in the community about this, I think it would help you all a lot and I think it would also improve the quality of the conversation in the community. So thanks a million.

[Applause]

GRAY CHYNOWETH: Thank you, Mikey. And thank you, everyone, for joining us today.

NANCY LUPIANO: Our next session on ethics will be starting very shortly. Ethics and conflicts of interest will begin very shortly. Thank you.