FTC MOBILE CRAMMING ROUNDTABLE
TRANSCRIPT
SEGMENT 2
05/08/13

RUSSELL DEITCH: Welcome, everybody. My name is Russell Deitch, with the Federal Trade Commission. I'm a veteran of the original cramming form here at the FTC, two years ago. It's almost our anniversary. And we dealt with landline cramming, and we raised the issues relating to wireless line cramming.

Today, we're going to get into current strategies reducing mobile marketing cramming. We have a lot to talk about, so I'm going to jump right into the panelists and issues. So take it away, Duane.

DUANE POZZA: So I'm Duane Pozza. I'm now a panelist. I'm a moderator. I'm at the Federal Trade Commission. We have a lot of great panelists. And they're going to go down the line and introduce themselves. And we've also asked them to give just a brief overview of--

DUANE POZZA: Sorry, we have some interference. Sorry about that. So at the risk of trampling over our panelists, I am one of the attorneys that is involved in the Wise Media case. We heard that reference various times in the introductory remarks and on the first panel.

This second panel is about the current strategies to combat mobile cramming. So just as a way of framing this and rather than going back to it throughout the questions, I wanted to just point out some of the facts that we learned in that case because that is a real time example of a cramming scheme that existed over the last couple years that sort of was an issue despite the current efforts to combat mobile cramming.

Just as an overview, the FTC sued Wise Media and its two operators in mid April. Wise Media purported to sell recurring subscriptions to regular text messages containing love tips, horoscope tips, billed at $9.99 a month. These are recurring charges. Wise Media claimed that consumers opted in on a website.

So the form of double opt in that they used was consumers go to a website. They input their phone number. Wise Media sends a text message to the consumer with a pin. And the consumers then input that pin into the website to complete the sign up. So that is what, as we heard on the first panel, would be one version of a double opt in process.

Wise Media then places the charges on consumers' phone bills by arrangements with aggregators. Consumers who noticed the charges widely reported they had never even heard of Wise Media. They had never been to the website. Some of them reported they don't use text messages. Some reported they were unable to receive text messages on the lines that were billed.

Additionally, consumers reported difficulties getting refunds. There's evidence in the record that carriers often sent them to Wise Media to get a refund. Consumers reported that they reached a

call center where they were promised a refund by Wise Media representatives. They never got one.

Wise Media's monthly refund rate, and this is something we'll talk about on this panel, by short code reached as high as 30% to 40% a month for short code. Carriers reacted in different ways. One carrier, in November, 2011 saw refunds around 40% in different short codes, and placed the campaigns on a watch list-- meaning that if refund rates persisted for another month, then they would no longer be able to enroll new subscribers.

Wise Media continued billing on that carrier through at least the end of 2012. Another carrier also noted in October, 2011, refund rates were 37% to 38%. And then suspended the short codes, continued billing on some of them for another six months, and then cut them off. In May, 2012, another carrier terminated all campaigns by Wise Media because it exceeded a refund rate of 8%. So that was the guideline at which they cut them off.

Overall, Wise Media was able to collect more than $6 million in 18 months. The carriers received 30% to 40% of the charges. Wise Media was able to place charges on more than two million phone bills. And consumers have received to date over 190,000 refunds.

Those are some of the numbers as a backdrop of a specific case study of what one of the-- and this is all public information, just to be clear. This is all public information in the record about what one alleged crammer was able to do. So with that said, I'd like to turn it back to our panelists, let them introduce themselves, and talk about their perspectives on what the current efforts are to address the mobile cramming issue. First up is Jim.

JIM CHILSEN: Hi, everybody. I want to thank the Federal Trade Commission for continuing the conversation on mobile cramming. My name is Jim Chilsen. I'm director of communications for the Citizens Utility Board, or CUB. We are a nonprofit consumer watchdog group that has spent the last 30 years fighting for better telecom policy in Illinois.

Last year, governor Pat Quinn used CUB's headquarters to sign one of the nation's toughest laws to combat-- landline cramming. That bill was championed by Attorney General Lisa Madigan, and it follows in the footsteps of our friends in Vermont. But now that our landline bills are under lock and key, CUB's concern is that scam artists have declared open season on our cellphone bills and that cell phone related commerce is the new frontier for fraud.

And that concern comes out of both experience and analysis. Last December, CUB partnered with wireless research from Validas to release an analysis of more than 200,000 Illinois cell phone lines. And we found that the number of suspicious charges had nearly doubled on Illinois cell phone bills from one year to the next.

Now Validas took a very conservative approach, only labeling charges as suspicious if it was connected to a company that had been involved in past phone fraud litigation. Our experience at CUB tells us that this analysis may just be the tip of the iceberg. We hold hundreds of phone bill clinics across the state of Illinois.

We see these suspicious charges all the time. We see suspicious charges on our own cell phone bills. I am not proud to say that I'm a victim of cramming. One of our top lawyers at CUB went three months before she realized she had a $9.99 premium services fee on her bill.

It was some type of love tips service called Love Genie. Now, Kristi is happily married. She's got a new baby. She had no business. And she did not order Love Genie. And by the way, Love Genie is offered by Wise Media, which the Federal Trade Commission just recently wisely sued.

It is encouraging to see the steps that the wireless industry has taken to combat cramming. But I do think it's inevitable that we will need tougher regulations to crack down on cramming. And that would include some type of ban on third party charges with reasonable common sense exceptions.

Now, no question there are legitimate third party charges. I am grateful that I was able to use my cell phone to give to hurricane relief. But I think we need tougher regulations to draw some clear lines between what is appropriate and inappropriate. And I think moving beyond self regulation is vital. Not only to protect customers, but it's vital for the health of the growing cell phone economy. And it's vital for the credibility of the cell phone industry. Thank you

CARA FREY: So I got excited because Cubs and Illinois. I thought we were talking baseball. But anyway, so my name is Cara Frey, and I am general council of the Mobile Marketing Association. The MMA is a global, not for profit trade association whose mission basically is to make mobile an indispensable part of the marketing mix. We represent all players in the industry.

So in the past panel, you kind of heard the description of each of the players-- so brand marketers, or content providers, enabling technology providers who are the carriers and the aggregators, and then sellers of advertising and marketing services. The reason we wanted to participate in this round table-- and I thank the FTC for allowing us to do that-- is to first and foremost state that we believe that mobile cramming is bad.

And I know that sounds extremely simplistic and obvious. But from our perspective, if mobile cramming persists and actually if it increases, that at some point the consumer is not going to want to participate in the mobile channel and the industry will shrink. And again, that's completely opposite of what our mission of the MMA is.

I also think we can offer some relevant history regarding our industry's efforts to establish clear guidelines for messaging. You heard Jim Manis. Jim Manis was the global chairperson of the MMA back from, I believe, 2003 to 2005. But back in 2005 when the mobile industry really was in its infancy, there were no rules for messaging.

So the MMA, seeing the need for this, brought together an industry coalition that established guidelines for messaging with the kind of three key elements being transparency, control, and choice. Those guidelines became known as the consumer best practice guidelines, and were approximately 14 pages long at that time. By 2009, those 14 pages had grown to about 150 pages.

And mostly that was because the common rules of the carriers were consolidated into that document. And then each individual carrier's guidelines were attached to that document. In 2012, the CTIA and MMA got together and worked to consolidate that 150 page document into 30 rules. And those 30 rules are what the CTIA is auditing against. And it makes sense for and for the CTIA to kind of take over those rules, those guidelines, because the MMA has never been an enforcement agency.

That's not what we are doing. We'll continue to work with our members to articulate best practices in mobile marketing in general, and including obviously messaging. And I do want to emphasize that I think we are in a unique position because we are the only trade association whose sole mission, or sole focus, is on the mobile industry. And because we represent all of the different players, I think we can uniquely influence the industry. And this gives us a perfect opportunity to try that. So thank you.

DEREK HALLIDAY: Hi, my name is Derek Halliday. I'm a product manager at Lookout Mobile Security. We're probably best well known for our consumer mobile applications-- one of which runs on Android, one of which runs on IOS-- that let people keep track and keep secure every aspect of their mobile experience. From backing up sensitive data, to finding a lost or stolen device, or to downloading applications, or browsing the web without fear of encountering malicious content.

And that last piece is what, I think, best fits into this conversation today. But first a little bit of context from our perspective. We have about over 35 million registered users at Lookout that span across 170 different countries and over 300 different operators. And about 50% of those new users we see every day are coming from international sources.

And what does that mean in terms of mobile apps? Well we see about roughly six million unique mobile applications out there in the ecosystem currently, and about 20,000 new applications each and every day that we analyze. So even at a small scale, the task that we sort of task our self with is figuring out which of those are good which are bad is somewhat daunting.

So one of the ways we actually do that is by deeply inspecting the content of an application. I guess the best way of thinking about is really thinking about it in terms of the genomic content of mobile applications out their and mobile app Genome Project.

And when we look at things like malware spyware, which are the biggest risks that pose threats to sort of our user base, the threats vary significantly by geography. In the US, it's really not a massive, massive risk of encountering malware. Just over 1% of US Android users encountered malware. Compare that with about four in 10 people who click on a fishing link, for instance, on their mobile device. It's pretty small.

But we continue see this trending upwards. And we see that fraudsters definitely recognize mobile as a major opportunity for monetizing their wares. If you compare the sort of rate of encountering malware in the US with places like China and Russia, for instance, it's a pretty stark contrast. The actual percentages of encountering threats there are 20% in China and around 40% in Russia. So it's pretty stark.

But when you look at what's responsible for that overall trend of malware in particular, we actually see it over 78% of malware threats are oriented around toll fraud. And that is essentially the lowest hanging fruit for some of these fraudsters. And in particular they're really not too sophisticated threats. They essentially worm their way onto your device by purporting to be a free game or service that may be normally a premium service.

Say I offered you a free Angry Birds Space that you normally have to pay $2 for. You might try that out and what actually happens is it might actually be a legitimate game that's fully functional, but behind the scenes it's sending text messages to premium short codes without your knowledge. And actually it can be able to intercept the response or double confirmation codes without your knowledge and responding in the affirmative to those. So they're very specifically designed to get around some of these safeguards that we have in place to protect users from this type of fraud.

In terms of how big of a draw this can be for some of these fraudsters, we estimated that on the conservative side one single family of malware that was designed to commit premium SMS toll fraud, netted upwards of $10 million over the course of nine months. When you look at the scale that mobile's operating at right now, it doesn't take much to really get those kinds of returns.

When we look forward to 2013, we very much feel that this is going to continue to be the top threat globally facing mobile users, in terms of what can harm their devices or their wallets. It remains an effective monetization scheme, especially in some of these areas where there's not nearly the kinds of regulations that there are in the US.

And there's actually been changes in the underlying platforms, for instance, on Android that have been designed to prevent this type of fraud. But those really aren't going to see the light of day in terms of mainstream adoption or penetration, at least for the next year or so.

So we're really glad to see people like MMA and the FTC get folks together and talk about this issue because when we look at the threats facing mobile consumers, this is really first and foremost among them.

JOHN BRUNER: Good morning and thank you for having us here today. I'm John Bruner. I'm the chief operating officer of Aegis mobile. Aegis mobile is a compliance and testing company that provides policing activities for the carrier PSMS market. Over the six years, seven years, that we've been in business is 2006, we've developed a life cycle approach to monitoring PSMS activity on carrier networks.

Mike spoke earlier from CTIA about the upfront venting process. The first thing we do is we do a background check on the companies that are intending to come onto a carrier's network for PSMS. We've amassed a database over the years that we've been doing that of good players and bad players that we're aware of.

We then move into functionally testing the product before it's released onto the network to ensure that it's compliant. What's nice about this phase of the process is that there are a lot of

content providers that want to do this is a valid business. And oftentimes what we will do with them is be helping them ensure that the program is compliant before it goes out onto the network.

Once it's released into the network, we've started with a baseline. The baseline says this content provider can get it right and is compliant with all of the requirements. But once it goes into the market, then we provide the media monitoring. We provide the functional testing in the market, all of the things that are done to ensure that the activity on the carriers' networks is staying compliant.

The third phase is that we pull post revenue data. And we pull data on the refunds, and revenue spikes, as well as customer care data. And we bring that into an integrated data warehouse that has all of our in market testing and all of our pre launch testing and background check. And we analyze that for activities that help us pinpoint and target bad behavior, and in addition go out and find it based on that data.

In every instance of our process, we're gathering documentation of everything that we do. All of that data is stored and all of that data is then presented to regulatory agencies and carriers to help prosecute and remove these bad content players from the market. Thank you.

DUANE POZZA: And just to remind everyone to speak into the microphone because the folks watching on the webcast, that's how they hear.

PAUL SINGER: Good morning. My name is Paul Singer. I'm an assistant Attorney General in the consumer protection division at the Texas Attorney General's office. I also thank the FTC for allowing me to be on the panel today. Real quick I'll say that any views expressed are mine and not necessarily those of the office of the Texas Attorney General, or Attorney General Greg Abbott. And nothing that I should be taken as legal advice today.

But part of the reason that I'm on this panel is that in 2011 our office filed a lawsuit against an Arizona based company Eye Level Holdings that did businesses as JAWA and several related entities and individuals. And essentially we alleged a highly sophisticated multimillion dollar mobile cramming operation. To give you a little perspective, these are some Texas numbers. In 2010, the full year before we filed seat, JAWA collected revenue from Texans in the neighborhood of $20 million with hundreds of thousands of subscribers in Texas alone.

In their court filings, they repeatedly asserted that they were making revenues in the neighborhood of a million dollars a day through PSMS billing. And they described themselves quite frequently as a billion dollar company. Many of my comments today are going to refer back to that case in large part because I think we learned a great deal about how some of this stuff is happening in the real world through that case. And we learned a number of lessons about the MMA guidelines and compliance standards.

And one of the reasons is that the company repeatedly asserted, and even post resolution of that case repeatedly asserted, that they were always and have always been MMA compliant. And I can touch on some of the interesting arguments that they made about the MMA guides and what they actually require.

And part of it is, and this is sort of a nice segue from the last panel, because CTIA talked about requirements for price disclosure, recurring nature of the subscription, and obtaining an affirmative opt in from a consumer. All of those happened with JAWA. And I've asked for a few minutes to walk through some slides and show exactly how it was happening so you get a sense of what was happening in the real world.

OK. So this is a sample program brief. This would be what was submitted to the cellphone carriers as a representation of what JAWA intended to be putting out publicly and advertising. Now one thing I should note, JAWA had hundreds of corporations that they registered using various employees within the company designated as the principal stakeholder for those corporations. And they set up mailboxes, private mailboxes, throughout the country as the registered address of each of those entities.

So from an application standpoint, every time they were obtaining a short code and submitting a brief to a carrier, it was through different entity with a different individual and an address that was randomly placed throughout the country. And you'll see in this program brief, there are some clear designations of what the price is going to be for the service. The short code is identified repeatedly on the brief itself.

So this is what happens in the real world. Consumers would get to a JAWA website first by doing an internet search for something that typically was offered for free-- so things like a movie showtime, or weather, or in this case funny jokes. And typically one of the first paid links that would show up would be a JAWA run website.

So once a consumer clicks through, this is a sample landing page of what they would get to. Obviously there's a very prominent call to action, asking for a consumer to enter their cell phone number. And there's little or no significant disclosure that occurs surrounding it. And this is one of these little examples where MMA requires a disclosure of the price.

To get into some of the nitty gritty, it needs to be 125 pixels from the entry of the cell phone field. Well in this case, you'll see that there is a reference here to monthly $9.99. It's buried in the background. It's blended in with this image. But on many of these sites, when you measure the distance between that and the cell phone field, it falls within that 125 pixels.

Once a consumer enters their cell phone number, as was described in the last panel, that serves as a first opt in for the double opt in process. A consumer was sent to a page that looks similar to this, asking them to enter the pin code that would be sent to them. Meanwhile, they would receive a text message.

One of the tricks that JAWA used was to insert large gaps of spacing in the text messages, themselves. So this a sample of an iPhone screen shot. And you'll see that when you open the message, this is what would show up, because it starts from the bottom of the text message. This is the language that you see. And all you see is the pass code down there at the bottom.

If you go to the top of the message, you see the same thing-- pass code. And then it's only if you actually scroll to the middle that you saw any reference to a price. And you'll see some monthly

$9.99 there. One other thing that I'd note, because this came up in the last panel too, you'll see this reference to standard rate plan in the text. That was actually the corporate entity that registered this short code and that was billing on the consumer cellphone bills. So on the cell phone bill, went in identified what this charge was, it red as standard rate plan.

Now one other quick note on how JAWA worked-- if a consumer ever went back and said, hm, I want to see what that web page looked like that I first got taken to. If they typed in the actual URL of the website, they would be taken to an entirely different page. And it would look something in the neighborhood of this a lot of times, which is just a non PSMS generic page, and one thing John may want to comment on, as well.

But JAWA used a fairly sophisticated cloaking technology where it would gather the IP addresses of the auditors. And when auditors would try to go through and check these sites, it would serve up a page that looked similar to this to the auditors, as opposed to seeing what was happening to consumers.

This is another quick example of an advertised web page, which you'll see on the left, and then what we call the direct page where the consumer or user would type in the actual address. And this was sort of another tactic that they used where you'll see that the pages, themselves, are very similar, but you'll see on the right the page where the consumer might go back and double check that at some point has far more prominent disclosures, many more price points. It includes a far more prominent check box at the bottom.

One final note on check boxes using this example. You'll see this is the actual consumer advertised site. You'll see that there's a check box under that cell submit field with very difficult to read language that was coloring blended it into the background. If the consumer entered their cell phone number and failed to check the box, a little pop up came up like this. It said select OK to go to the maps. And if you click OK, it checks the check box and takes you to the next step. And it would actually treat it as your first opt in.

By comparison the page when a consumer would directly type in the website, if you didn't check the box, you got this alert that told you that you have to go back and accept the terms and conditions. And it would simply take you back to the initial page in order to require you to physically check the box.

So I mean that's just my quick demonstration. Like I said, I'll be referencing back some of the lessons that we learned in this case and some of the examples from it.

DUANE POZZA: Plenty more to explore there. Our last panelist is actually participating by phone. It's Chris Whitman, senior staff counsel at the California Public Utilities Commission. And, hold on a second, I will get a him on the phone.

CHRIS WITTEMAN: I'm here.

DUANE POZZA: Are you there, Chris?

CHRIS WITTEMAN: Can you hear me now?

DUANE POZZA: Yes. I'll let you know if there's any feedback. You might have to mute your webcast.

CHRIS WITTEMAN: OK. So my name is Chris Witteman. I'm an attorney with the California Public Utilities Commission. And I should follow immediately with the same disclaimer that Mr. Singer made. I am here speaking for myself and not for the California Public Utilities Commission. I have participated in a number of proceedings there that involve cramming. So I have some idea about this subject.

And I do want to thank the FTC for having this panel and for having me on the panel. We, out in California, very much appreciate the FTC's efforts in the cramming area. Particularly the Inc21 case in the Northern District of California was a seminal case for us on the west coast.

The second substantive point I'd make is how little we know. As referenced in the first panel, the mobile and wire line third party billing ecology is a three legged stool. You have the billing telephone companies. You have the aggregators and you have the service or content providers. And this version of rules leads to, from my perception, some lack of accountability on the part of each of the carriers.

And as the Vermont Attorney General said, a gap between rules and reality. What we have done in California to address that issue is a decision and rules issued in 2010 around cramming and the light motif of that decision is this sentence-- the billing telephone corporation bears ultimate responsibility for all items presented in a subscriber's bill.

With that principle, we have required billing telephone companies to conduct a reasonable inquiry before they sign on a service or content provider. Before they give billing privileges, if you will, to a service or content provider, we require the billing telephone corporation to disclose the possibility of blocking third party charges. We require the billing telephone corporation to report refunds to us.

And we use refunds as a proxy for complaints because when we had complaint reporting, we will end up in endless semantic digressions around the meaning of the word complaint. So refund is something a little more tangible. And we assume that in most cases, refunds are not made out of the blue but in relation to some expression of dissatisfaction by the customer.

And finally, we require billing telephone corporations to resolve complaints and to terminate bad actors. In the area of complaint reporting, I understand that our letter to the Senate committee reporting refunds in the wireless space will become part of the record. And you see there that what the carriers are reporting to us is a refund rate in the area of 12% or 13%.

So this begs the question of, what is the threshold for terminating bad actors in this space? Is it 8%, as we heard in the previous panel, or is it something else? The other thing that you can read out of that letter and the data provided there is how small the complaint numbers, to us as an

agency, are in relation to the refund rate. And we suspect that the refund rates, themselves, are small in relation to the total volume.

I was interested to hear Mr. Singer's discussion of his recent case. We, in California, have been litigating and are still in the process of litigating a case against Tell7 and Calling10. In that case, there were two to three million Californians who were charged $7.70 roughly for supposedly directory assistance. We did not find one customer, could not find one customer, who admitted authorizing that directory assistance charge that appeared on bills.

There was an opt in there, or a nominal opt in, by virtue of the consumer calling supposedly to get this directory assistance. But we believe that was induced you might say fraudulently or by misleading the statements in the context of the call.

So the final thing I'd like to discuss, in terms of strategies to reduce mobile cramming, is the bill blocking option. That is one of the things that we require of billing telephone corporations, that they disclose that, and that there is that option. The question then becomes, how well do they disclose this? And our preliminary investigation of this leads us to the conclusion not very well, at least not in all cases.

In many cases, consumer service reps are unaware that there is a bill block option. It's not prominently featured on websites. And the mechanisms of adding and removing the blocks, which this should be free per our rules, and should be easily added and removed. Those mechanisms are not always clearly described. So that's the landscape from our perspective.

DUANE POZZA: Thanks, Chris. So, turning to some open ended questions. One topic that we want to drill down on is the vetting of content providers. As we heard in the last panel and then in the introductory remarks about the efforts that different players in the industry make to vet the content providers-- and this again are the companies actually providing the horoscope, or the content, or the ring tones or whatever-- and placing the billable event on the bill.

So just to kick off the discussion, how much upfront vetting is really done before a content provider can start billing a consumer? And how robust is it? And then the second half of that is once it goes live, how much followup is done? On the first panel, Mike Alcho said something to the effect of that carriers touch every code, every month, or something, not to misquote you, Mike. But just drill down on how often and how robust is the vetting once these companies are actually putting charges on the bill. Maybe we could start with John.

JOHN BRUNER: Sure. I'll stay on the microphones this time. So to define vetting first, because I think Duane and I, when we first started talking vetting, that we were using it differently. Vetting is actually doing a background check on the content provider that wishes to come onto a carrier's network, or wishes to purchase a short code through CTIA first.

The vetting process is essentially a background check much as you do a background check on an individual for a credit card. We seek databases that we pay for, as a company. But we also do a number of other data sources, which I'm not going to disclose all of those data sources at this time, simply because it is part of the secret sauces protecting this industry.

But upfront, we do that complete check. And if we find anything that number one associates that content provider with any bad behavior in the past related to cramming, any open lawsuits, any kind of articles talking about that company. But in addition, any relationships of any of the people within that company that play key roles, or any of the other features of that company that they submit. And I'll say very vaguely bank accounts, addresses, at the highest level, we can connect those to people that we've vetted in the past and more importantly companies that we have removed with their carriers from the network.

So I have a slide that I show sometimes that I pictorially shows groupings of bad players, how they come back as different companies and turn bad. But you'll see, when we plot them on a point diagram, that you have clusters of good players that have relationships to each other. And then you have clusters of bad players.

And sometimes what we find is we'll find clusters of bad players and we'll find a few not yet bad players related to them. And so in terms of going beyond the vetting, that's one of the indicators that we use to two more closely monitor those companies that seem to have relationships with other companies that we've found in the past.

When Paul talked about the Arizona based company earlier, they had hundreds of companies associated. And they were playing the shell game. You play bad this week, and then we'll send it over to another company to play bad next week. For that reason, when we do our vetting, we're looking at of the doing business as names and all of the relationships of all companies that are associated with the company applying. And again, that's all stored in a relational database. And we use it, and we leverage that data as another source of identifying bad behavior.

DUANE POZZA: And how much of the monitoring is ongoing in terms of compliance to the MMA guidelines? And is that the touchstone for monitoring content providers once they go live? And is that enough to ensure that these content providers are not engaged in deceptive or cramming behavior?

JOHN BRUNER: We actually believe that the full life cycle approaches is critical. And the ability to join the data across the full life cycle is important. One of the things that I probably failed to mention in the first answer is that companies change. So just because you've vetted them once to let them onto the network, doesn't mean that they acquire a new CEO or they acquire another company.

And so re-vetting is also a very important thing. A couple things that we will do is we'll put crawlers out looking for changes that are occurring to companies. One of the things that we will do is we will re-vet on an annual basis. One of the things that we will do is when we find advertising or any sort of information out on the network that tells us that a company had come into risk because of some change in the company, then we go back to our customers and recommend a re-vet, just to make sure that they stay good players.

In terms of jumping into the market, yes it's very important because that's the other side of it. Companies will change potentially after being vetted. And they change all the time. And so to say that they can get through and get on the network and pass the vetting process doesn't mean

that they won't then start doing deceptive advertising, stack marketing, and anything they can do to get people to buy their products without them necessarily understanding what they've done. So the monitoring is very important.

The monitoring all of the advertising and ways that link into the process of purchasing on PSMS, as well as the functional testing and the content testing. As well as then analyzing the billing that comes in to ensure that the bills face descriptors are accurate. As well as looking at refund rates, which we've heard a lot, as well as looking at revenue spikes. As well as looking at activities when, for example, a catastrophic risk occurs, because bad guys come out of the woodwork when there's an opportunity. When everybody's willing to donate money, then that might be a bigger opportunity for them to get things. I'm not saying the charities aren't the safest things that we see in the PSMS market. What I'm saying is it's another opportunity.

So all of these have to be taken into consideration. One of the things that Paul said earlier about how some of these bad guys are using the alternative good site when they know who you are coming in as an auditor versus the site for the unsuspecting, that's true. That's a fact. It happens. As a matter of fact, we prefer when they do that because we can find both. And that's direct evidence that they know what they're doing. We can show that they have one site that's fully compliant and another site that's not.

So part of the tactic, obviously though, is these are smart technology companies. So the best thing for us to do as a company is to stay ahead of them, technically, which means we're continually evolving what we do to monitor their behavior.

RUSSELL DEITCH: One of my favorite terms is room for improvement. And I've heard situations where different carriers have different refunded charge back rates. I'm wondering if the cramming problem could be improved if there were an adoption of lower threshold rates by all carriers, or sharing of bad actors between carriers, so one could not jump just to the other. What do the panelists think about those types of approaches to reduce cramming, and what kind of impact that would have? Cara, do you want to start with some initial thoughts?

CARA FREY: In all honesty, I don't have much information on that issue. I think, in all honesty, that's probably best asked of Michael. So again, from the MMA's perspective, I think John just said technology is evolving at such a quick rate. And the industry really has to keep up with it. So anything that, I think, we can do to try to keep up with that and really address these bad actors.

I keep hearing talk of bad actors. And really at some point, it's obviously fraudulent behavior. And so I encourage, and from the MMA's prospective, we would encourage that these entities-- and there are multiple entities out there-- be prosecuted. And I love personally hearing about these prosecutions because I think that's going to be what inevitably has to happen.

RUSSELL DEITCH: John, if everybody adopted more aggressive procedures, and if the carriers ratcheted down thresholds for refunds or charge backs and shared information, do you think there would be an impact on cramming?

JOHN BRUNER: That's kind of outside of my purview, though, because I really leave it to carriers to determine how they want to make their a refund rates. I'll say more generally that you probably need to look at the amount of revenue before you look at the refund rate as a relationship. Because you could have something that launches that's got $100 a month coming on it, and it's got free refunds. And so they're at 30%.

I think you need to take a little more into account than refund rate, which is kind of like we like to take into account the data regarding customer complaints, the help desk, as well as the refund revenue data. As well as looking at the bill face descriptors. As well as doing the in-market monitoring. I'm kind of dodging it, but to me a carrier should be answering that.

DUANE POZZA: What do other folks on the panel think about what would be a good refund rate that would seem like it would signal that the potential bad actor that some action should be taken against? And I'll just note that as one benchmark, I believe Jim Manis said on the first panel that they saw a refund rate of around 1% to 1.5% on the charitable side. And in the credit card context, it's generally below 1% is the threshold for fraud.

CHRIS WITTEMAN: This is Chris Witteman out in California. In the Tell7 case, we saw a refund rate really very low, about 5%. And that gets to the point made earlier that 80% of customers may not even be aware that they are potentially being billed by third parties. So I think we need to look very closely at this question. And I think that the rate should be on the low side. 5% would with definitely send warning signals.

Also on the question of vetting, we've heard for years from the industry that they are vetting. And when you actually see the documentation of the vetting, and I look forward to seeing documentation from AeGIS and groups like that, but the documentation we've seen has been a pro form of boilerplate check the boxes form that the content provider will fill out and provide to the aggregate who then provides it to the billing telephone company.

So I'm skeptical about the upfront vetting. And I'm skeptical about the refund or complaint threshold required to trigger serious scrutiny.

PAUL SINGER: I want to say two things real quick about refunds. One, you obviously have the risk of a JAWA like situation, right? Where you had multiple entities set up in large part to keep refund rate at an incredibly low threshold. And so it was very easy for them to just transition the exact same program from one entity, one short code, and an escalating refund rate to a brand new one, where you now have this seemingly new entity that is sort of starting from scratch.

The other issue, I think, is that refund rate necessarily implies that people are actually successfully in getting refunds. And I think that the Vermont survey consumer complaints, they all reflect a lot of varied experiences on consumers actually obtaining meaningful refunds. And just one example from our litigation,

I'll up Jim a little bit. But one of our investigators in our JAWA case, six weeks into the investigation, he comes in my office with his head hung low and realized that he'd been crammed

for 11 months by them. And it took him that long to even realize it after we had been looking at them. He had multiple calls with this carrier attempting to get a refund.

First was told no, he can't get any refund. Next he was given either two or three month refund. Ultimately the only way you got a full refund was to go to JAWA directly, who maintained a full, no questions asked full refund policy, and issued have made a full refund.

JIM CHILSEN: I'll give Kristy's-- maybe we can get his number and Kristy and him can cry on other's shoulders.

PAUL SINGER: They can swap text messages.

JIM CHILSEN: It does feel like it's just one big game of high tech whack-a-mole. And there was a New York Times article which was referenced in the first panel, which talked about double opt in and all these great guidelines, which are excellent. But guidelines work best when the players are honest to begin with, I think. And that's one big problem is that good guidelines, I think, are no replacement for tough reasonable regulations.

RUSSELL DEITCH: We have a question from email. We're part of the high tech group here. We might as well get high tech questions. It deals with the overlap between landline and wireless billing. As they say, those who forget history are doomed to repeat it. When we had our cramming form two years ago, I remember some of the stories.

The Illinois AG talked about credit repair charges on a central public library story line, which was a pre-recorded line. The same credit repair charges showed up on the county coroner's office bill. And by the time you're at the county coroner's office, I can't imagine you're worried about your credit rating.

RUSSELL DEITCH: And subsequently the FTC filed a comment with the FCC on landline cramming. And just the topics are abuse of the third party billing system is widespread. There's a scarcity of evidence of legitimate use of third party billing. Disclosures are unlikely to be noticed and will not solve the cramming problem. And the FCC should ban a required default blocking or some or all third party charges.

So the real overwhelming question is, what can we learn from landline billing? And that's a long lead up to the question which is, when there's vetting in the mobile billing space, are vendors asked about their history if any in landline billing? If so, what is asked of them? So John, you'd probably be the first person to respond to that.

JOHN BRUNER: I'll say the answer is no, we're not asking them specifically if they were ever associated with any landline cramming. Our investigations, though, of the 40 to 50 data sources that we check has revealed content providers that were associated with cramming on other types of channels.

RUSSELL DEITCH: And the bigger question for the panelists is, what lessons can we learn from the experience with landline cramming?

PAUL SINGER: Well, I think you hit on it earlier. One of the questions has to be, what's the actual content that's being billed for? Is this content that consumers are likely to be knowingly choosing to purchase? Or is this something that's widely available for free, and it's very unlikely that they would be purchasing this?

I ran through some of the different categories of things that JAWA was marketing. All of them were widely available for free. And in fact, in their customer service calls that they wanted to use as evidence of their very generous refund policy, there were repeated references from consumers saying, well I would have never paid for this. Why would I pay for the service? It's available for free. So I think those are legitimate questions to be asking because it's certainly something that happened historically on the landline side.

DEREK HALLIDAY: And at the same time, that's somewhat complicated by the fact that there's so many new types of services that are embedded on mobile that don't exist on landline. The entire app ecosystem, for instance, doesn't have any kind of corollary in landline space.

And so there is, however far fetched, a very legitimate use case where someone is paying $1.99, $2.99 a month for a horoscope that's delivered by an app on their mobile device. As much as I think people in this room probably wouldn't be subscribing to that kind of service, it is a legitimate use case with things like premium apps.

So that, I think, provides an additional layer of complexity to this issue, in mobile specifically. I think that, going back to some other things that we just talked about in the last question, there are a bunch of different options we can use to actually correlate some of these bad actors in the mobile ecosystem that help us sort of cordon off potential bad actors, including things like reputation.

So while the issues become more complex when you throw things like applications into the mix, it does provide us a number of different, additional levers to correlate and identify say the same bad actor playing this shell game jumping from developer to developer, for instance.

DUANE POZZA: I want to ask a follow-up question. A lot of this discussion has been, how do catch the bad actors? Which we should talk about more. For the actors who are not just being totally fraudulent and are claiming to respond or to comply with Consumer Best Practices, or MMA guidelines as we've talked about, what is the process going-- are those guidelines sufficient right now in the world of third party billing on mobile services?

And what is the capacity for input to improve them? Is there? Are they evolving? Are they flexible? And how will they evolve over the next few years? So, Cara.

CARA FREY: I'll start. So again, I think we all refer to them as the MMA guidelines. But in fact, they really are the Consumer Best Practice Guidelines. And as I kind of explained in my opening, what those guidelines became really were the carrier common rules. And that one document, the Consumer Best Practices, really provided one place that people who are running marketing campaigns can go to access all the information.

And as I explained, in 2012 version seven of the CBP guidelines was actually the last version published. And now, the CTIA-- like I said, the MMA and the CTIA consolidated version seven into 30 rules, which I think really is helpful. Because those are the most basic, necessary rules. And CTIA now and has been auditing against the guidelines and now those rules and will continue to do so.

Obviously, like I said, I think this is all part of an evolution. But I think the rules are very effective. And I think, to be honest I don't want to particularly get way into self regulation versus government regulating, but I do think that there is a very positive element of self regulation that we can act, as the industry, much faster than the government can act. But I do think that the rules will continue to evolve and the CTIA will continue to audit against those.

And I would assume, again, the MMA has really stepped out of the space of drafting guidelines. So I don't want to speak really totally for the CTIA, but I would imagine that they will continue to monitor these the rules and continue to draft more if they're necessary.

DUANE POZZA: Other thoughts on the panel?

PAUL SINGER: So, I think there's a couple of thoughts. One is, in our litigation, we heavily use the rules-- in large part because we looked at this as, hey, industry is attempting to self regulate. Let's look at those standards. And let's see whether or not this company is even compliant with that as a floor to sort of what should be a proper, clear, and conspicuous disclosure under our state UDAP law.

And I think some of the complications of it art that one, the MMA guide, CTIA, whoever's monitoring, they do get into the weeds somewhat, right? You have a lot of very detailed, specific-- I mentioned the one before about the price disclosure, 125 pixels from the cell phone entry field. I think the more detailed you get like that, the greater the risk that you lose sight of the big picture, which is that these still need to be clear and conspicuous.

And they need to be adequately disclosed to consumers so they understand what they're signing up for. And I think one of the interesting pieces is that MMA historically defined clear and conspicuous as referencing back to the FTC.com disclosures as sort of a good standard and something to look at. And when we questioned JAWA representatives about those disclosures, they didn't know what they were. They had no idea that those were there. But they certainly knew there the detailed auditing requirements about trying to put a price point 125 pixels from a cell phone entry field.

I think the other comment I'd like to make about the rules is that there's always room for improvement. One of the things that we looked to when we were crafting a final permanent injunction in our JAWA litigation, was how can we take the rules and make them clearer and more expressed that you don't have companies who can try to use creative interpretations of those rules to get around them.

And just another quick example. I showed the text messages that JAWA used. One of the rule says that the pin has to be after the price in the text message. I'm paraphrasing, but that's

generally how that's worded. What it doesn't say is that the pin can also be before the price, which is what JAWA was doing. So you had pin at the start, pin at the end, and price somewhere buried in the middle. So those are examples of there's always sort of room for improvement and sort of looking at the way companies are creatively interpreting these rules.

CHRIS WITTEMAN: This is Chris Witteman out in California again with a question for MMA or CTIA, if that is the body that's enforcing this. Would they commit to an open door policy vis a vis state agencies and the FTC and the FCC so that we could see where their concerns were and what their enforcement efforts were.

CARA FREY: Yeah. This is Cara from the MMA. But the MMA has never been an enforcement body. So I can't address that.

DEREK HALLIDAY: Actually, I wanted to jump in on this one, as well. As a mobile standpoint, someone as the consumer advocate from a security and privacy standpoint on consumer devices, having a clearly established set of guidelines such as these is immensely important. And having those guidelines be extremely clear is just as important because we view ourselves as somewhat of an opt in enforcer for some of these guidelines, themselves. The example that we've been most familiar with in the past year

has been very similar to this. But working with MMA to figure out what the right guidelines are for the collection of PII from mobile devices. So I think it's very similar to this issue. And it provides a framework for ourselves, as a security company that scans the apps on your phone, to tell you what you might want to be concerned about.

And so for companies like ourselves that are there to protect the user and inform them and keep them informed, I think there's a clear need for these types of guidelines. That said, I think it's essential that a consumer advocate or watchdog is extremely involved in shaping those guidelines so that they're not done in a vacuum. Because certainly you can iterate very quickly at speed on some of these guidelines all you want, but if you're not actually addressing the concerns that are facing users and addressing the right bar of risk for users, you're not going to get anywhere.

JOHN BRUNER: If I could add, the carriers that we represent in the in-market monitoring do also have and have added rules of their own to that. One that comes to mind that's even most interesting to me gives our testers the ability to raise issues when they can't necessarily pair a problem directly to an MMA/CTIA rule. And so we have seen the behavior where carriers are actually enhancing the rules to get greater opportunity to catch what could be bad behavior.

CARA FREY: And Paul, to your point that the rules really seem like we're getting into the weeds, you are absolutely correct. I sat in meetings where I can't even begin to describe

how many weeds we were in. And that really, I think, in 2012 when we decided to hand it over to CTIA and create just the 30 rules, I'm hopeful that will get us out of the weeds and be helpful to the industry. But I totally agree with you.

JIM CHILSEN: I'd just like to add that I think it's important to say that good, solid guidelines and government regulation should not be mutually exclusive. They can work very well together. And when I hear Paul talk about that case in Texas, I hear diversionary software, shell corporations, sophisticated cloaking software, and I think guidelines alone can't meet a formidable foe like that.

RUSSELL DEITCH: Let's move in a little bit different direction. There are three, big components of any online transaction. There are the disclosures. There's this term that keeps getting bandied about, the double opt in. And then there's consumer's ability to dispute charges or get refunds.

Since we've heard this double opt in term so often, is there's somebody that could explain what it means and the alphabet soup that goes with it? We hear WAP billing, wireless access protocol, premium SMS. And from there, I'd like to get into issues or problems with double opt in. So could somebody educate us exactly what double opt in is and how it works?

JOHN BRUNER: Double opt in is the point at which a consumer commits to a purchase. The process is designed to ensure that the consumer knows exactly what they are purchasing. And the second opt in is to reconfirm. The text message goes out to the consumer saying you've agreed to purchase this. It's all designed to ensure that the consumer knows what they're doing.

To add to that, though, I would say that what we see in the market is not a violation of the double opt in where it's being skipped, necessarily. What we see is consumers are, either through stacked marketing or deceptive advertising, double opting in and not realizing that they had purchased something. And so the physical process, itself, seems to be a very sound process for purchase. It's more the method leading up to getting a consumer to perform that function.

RUSSELL DEITCH: Let's follow up on that. Giving us a scenario where the initial disclosures are deceptive prior to the opt in, if we look at the next component, what does the opt in actually tell you? Do you get a receipt? Do you know who's-- with what billing, usually there's two pushes on a button.

Do you know who's actually pushing the button? Could it be the line subscriber, a child, or somebody else with your phone? And the same situation with a pin-- are there issues when it comes to authentication and receipt with the double opt in? Are there ways to improve that?

DUANE POZZA: Well, one question to frame that is, maybe get some clarity, who has the records of the opt ins? And who has access to them? And can there be an improvement in that regard?

RUSSELL DEITCH: And what are they?

JOHN BRUNER: I think you've got the wrong panelists because that's really an aggregator, carrier, content provider relationship. I'm a third party--

CHRIS WITTEMAN: Out in California, we have looked into that a little bit. And contrary to what was said on the first panel, it's our understanding that those records reside only with the service provider. They're not even provided to the aggregator.

So one possible solution or measure that could be taken would be to make sure that the aggregator had access to those and that the billing telephone corporation had access to those so that they could look into those records and see a, if they're there, and b, if they're credible. And like I said earlier, in the Tell7 case, we had the functional equivalent of opt in evidence, but it was our conclusion at the end of the day that had been fraudulently obtained.

RUSSELL DEITCH: And let me ask another question getting onto remedies. Are the current remedies available to consumers sufficient? We've heard discussion on how people may not know that charges, or third party charges, are even going to be on their cell phone bills. We've heard discussion that the charges may be small, may be difficult to find. There are the whole issues of automatic bill pay, or even prepaid charges. Is there more that can be done to make the refund mechanisms adequate? Or is the status quo acceptable?

CARA FREY: Before we get to that, I did want to respond to what was said over the phone. And I've heard the suggestion that opt in management should be maybe brought in-house, or kind of moved up the chain. But one thing that I want to put out there is that these major brands, the content providers, see that as proprietary asset.

So I would wonder and ask the hardcore lawyers-- I don't like to think of myself as a hardcore lawyer-- what's your response to that? How do you protect that proprietary asset? And also, just to throw out there, I do think there needs to be this balance.

And I don't know where the balance is, but between innovation and a lot of regulation. I think we have to really keep that in mind as we discuss all of this. But I am interested on the proprietary asset question about the opt ins.

DUANE POZZA: Do you want to ask a question about-- going back to Russell's questions about remedies, are those sufficient now? That consumers can have a remedy if they discover they're being crammed-- do they need to be improved? And what is the experience the panel has with that?

PAUL SINGER: So I talked about that a little bit earlier. I think the Vermont survey is the most recent example that's out there. No, remedies are often hard to obtain in this field. Consumers report all sorts of varying experiences about their ability to get their money back at the end of the day.

And the JAWA experience we had is just a really good one, where carriers were very resistant to the idea of telling people, go to try to get a refund, despite the fact that really was the only source to get a full refund at the end of the day. It, I think, demonstrates that there is just a great deal of variance in what's going on today in the marketplace. And consumers are having varied experiences that often with the result that they find it difficult, if not impossible, to ultimately get their money back.

RUSSELL DEITCH: Well that leads to a follow-up question. What can consumers do to protect themselves in the current environment with wireless billing?

DEREK HALLIDAY: Well, I would jump in, what Paul just mentioned, as well. We ask ourselves if the options for remediation or refunds are sufficient. And throughout this entire panel, we've been talking about the fact that one of the most difficult parts of this process-- the critical parts of this process-- is depending on a user to notice in their phone bill that there's an additional charge that they may not be aware of.

If you ask me, one of the most critical areas that's broken here is that exact process, is depending on the actual users, themselves, to notice in the 10 page phone bill they might get, that there's something they don't recognize. I think there's plenty of options for notifying users of these types of services beyond just an SMS based double opt in that operators have at their fingertips.

They're in constant communication with these users. Why not also send them an email notification? Why not go beyond just a simple SMS transaction to make it very abundantly clear that they're signing up to be charged? And not depend on them to actually initiate this process.

PAUL SINGER: And to add to that, it's understanding just fundamentally that you can be billed for third party charges through this mechanism. And I think the Vermont survey spoke very well about that being a major issue right now. The consumers just don't even understand at the outset that that's possible.

DUANE POZZA: What are the reactions of others on the panel, this idea that there would be some other notification, or even a different kind of notification on the phone bill or email or something like that, to a third party charge?

JIM CHILSEN: I think that's an excellent idea. What we've been asking for years is, can the cell phone industry create some type of red flag system like the credit card industry has. A couple years ago, there was this strange purchase on my bill. And I got a call right away, the credit card company wondering if that was legitimate. We would love to see something like that.

Right now, the best we can tell consumers is beware of any websites that ask for your cell phone number. Go to SMSwatchdog.com if you get a strange text to find out what you can do. But oftentimes, different people will say different things on that website. I replied stop and I still got the charge. Or I ignored it and I got the charge.

So it can be very confusing. At the top of the list is always for consumers, even in this high tech era, one of the best protections is just to make sure to read your bill-- your cell phone bill-- every month.

JOHN BRUNER: I'm not going to claim to be an expert in this space. But I have seen on a phone bill for a landline charge a statement separated out that this is a third party charge. Nonpayment of this charge will not result in termination of your service. And so for me, that stood out very plain and clear that this was not a charge from my carrier.

JIM CHILSEN: And just to add to that--

CHRIS WITTEMAN: One way that customer, consumer awareness might be raised is to go a little bit beyond the California rule, which requires disclosure of the blocking option, and to have an affirmative opt out. In other words, when the billing telephone corporation signs up a customer, that customer has to check a box or initial box that says, you may be billed by third party customers. Do you agree to that? I think that would be one step that might raise consciousness a little bit.

DUANE POZZA: Jim.

JIM CHILSEN: That's an excellent point What I was just going to add to what John said is what we tell people is if they find a suspicious charge their bill is to immediately call the cell phone company. And we also find that it helps to call some type of government entity-- the Illinois Attorney General's office, or the FCC, or the FTC-- just to be able to tell the cell phone company, I have this strange charge. I filed a complaint with a government entity. That seems to add. It might light a fire under the company.

And also to tell them I'm not going to pay this charge. It's under dispute. And I won't pay this charge. I'll pay every other part of my bill. And we can agree on the phone what that part is and what I should be paying. But I will not be paying this charge.

DUANE POZZA: Just following up on that-- do consumers have an understanding and is it the case that they can dispute a third party charge on their bill without having their phone service cut off?

JIM CHILSEN: No. I think I think that is a big-- and we try to educate people about that. You're not forced to pay this fee. And I think that's what happens a lot. And it's not just in the cell phone industry, it's across the-- we deal with charges on gas bills and landline telephone bills, where people think a charge is a required charge. It's not optional.

And they think they have to pay it. And then they call us after paying it for many months. And then it's much more difficult to get a full refund.

PAUL SINGER: Can I throw out there-- I want to back up to a question you asked earlier because I'm not sure that there's been really a complete answer about the various ways that the double opt in can occur. I think it would be really good. John, I'm going to sort of turn to you.

Do you mind just sort of running through? Because the JAWA example is just one of the various mechanisms in which a double opt in can occur. That was a web-based, cell phone, pin entry process. I was hoping you could just sort of run through the different ways that people can be opted in.

JOHN BRUNER: OK. Thank you.

PAUL SINGER: You're welcome.

JOHN BRUNER: I'd really like to, if I may, refer to an expert on the floor. Jen Sizer is a lead analyst in our organization who was very instrumental in the research and discovery of the Cylon/JAWA investigation. Jen, would you mind giving the various examples?

JEN SIZER: Thank you, John. Is it working? So we have phone opt in, which is a lot of what the charities use, where the text is originating from your phone. So you send a keyword to the company. The company responds back and asks for you to confirm that usually responding with yes or y. So that's a phone opt in.

Then we have the web opt in, which is what we were discussing with Cylon, where you enter your phone number on a website, and that's your initial opt in. They then send you a text message, which would send you either a pin or you can respond affirmatively with a yes or OK.

Then we were discussing WAP opt in, which is a little more outdated at this point. But it is directly on your handset where you double click. You'll get a pop up message that asks if you want to incur these charges. And you click yes twice.

Direct carrier billing, which is very similar to WAP, but generally doesn't involve the PMS charges. That's more of the Android applications, iPhone applications, where you're confirming that the bill will go, or that charges will go, onto your credit card or iTunes account.

Then, I guess the last one would be IVR, which is interactive voice response, which is where you call generally a toll free number. And they give you the details of the program on the phone before you then hit a button. Generally you press one to confirm that you want more information.

Then they're supposed to give you all the upfront details regarding the pricing, who to call for help, and require second key press prior to opting you in. And that's more prominent with chat programs and things like that. So I think that covers everything that you asked.

DUANE POZZA: Just to clarify. So in that there is the capacity for someone to push something on their smartphone twice, opting in, and the technology pulls the phone number off the phone and then bills to the phone number? Or is it more complicated?

JEN SIZER: I don't actually know the answer to that. The billing is occurring within the carrier and the aggregator. But I know that the key press generally is. Those are the two opt ins. So I assume that they have record of that.

RUSSELL DEITCH: And just to follow up on that, does it work where you have to push a buy button to do it twice? There's that specificity in MMA's guidelines.

JEN SIZER: There has been that specificity. I'm not sure exactly, right now. But I know that there was very specific terminology at one point that stated that you want to buy the product or order the product, not just click OK.

DUANE POZZA: OK. Thanks. We appreciate you being put on the spot.

JEN SIZER: Thank you.

DUANE POZZA: One question from the audience-- unless there are more follow ups to that-- one question from the audience is also about this double opt in process. How do you ensure that it's a consumer who's opting into the double opt in and not a content provider that's essentially submitting a charge and fabricating the records?

And I would add to that, going back to Derek's example he said at the beginning talking about toll fraud, these apps that I guess can sign you up without you even knowing it by sending a text message from your phone. Is there any technological way to differentiate those kinds of opt ins that are fraudulent from real opt ins?

JOHN BRUNER: Is that question saying that a content provider would take on the identity of a subscriber's telephone and opt in and buy something?

DUANE POZZA: Is there any technological barrier to that happening? That you see, obviously.

JOHN BRUNER: Unfortunately, that's all in the infrastructure between the content provider, the aggregator, and the carrier. It's not an area that Aegis mobile touches. We haven't seen that, though. You might have a good answer.

DEREK HALLIDAY: In the case that I referred to at the start of comments here, my understanding is there's no technical way of differentiating from the carrier's standpoint. Essentially because the way that these threats operate, we all know how mobile apps can ask for permissions.

So when you download a new app on your Android phone for instance, you go through a screen that says, this application requires or asks permission to access the internet, or to send text messages, for instance. So if an application of this sort asks for these types of specific permissions and you grant them those permissions, they have the ability to send text messages really however they see fit.

So in this specific instance, we've seen cases where malware is designed to recognize specific in-bound text messages that look like double opt in messages. And basically get in front of your standard text message application on your phone before you see it. And then respond directly from your phone. So from a carrier standpoint, they can't tell whether it's something you originated or an application originated.

PAUL SINGER: And one other example, too. One of the methods to enroll, you don't need to do anything from your handset. The web-based pin entry doesn't require the consumer to affirmatively do anything from the actual handset. Well, the folks at JAWA/Cylon had sort of run afoul of this before they developed this system.

The first system they developed was when you would get to the pin entry page, they would both send you a text message and then post the pin on the website, so that whoever was doing it could just write the pin in directly there. So there was really no way to verify that it was the actual

consumer who was receiving the text message that was entering it. It could just be anyone who was going to the website. So there are certainly ways to circumvent the process.

DEREK HALLIDAY: Yeah. Not to get too technical, but in some of those cases, you have at least a little bit more evidence that you can potentially correlate. IP addresses that are there assigned to give an end point devices in a network you can correlate back to specific subscriber's identities.

So it takes a little bit of effort, but you can get down to the bottom of it. When it comes to just text messages and threats or fraud that is actually on your end point device, it's impossible to really discern.

DUANE POZZA: Since this is actually involves asking the aggregators, we have a representative from an aggregator in our audience who wants to chime in. So, Allen.

ALLEN: Thank you.

DUANE POZZA: He's actually on the next panel. But we'll give him the floor.

ALLEN: Yeah. Everyone please stay after lunch, if you really want to get the really good stuff. But there were two questions that arose that I believe are properly placed to the aggregator. I'm with a company called M Cubed Incorporated, which is one of the larger and longer-lasting aggregators for commercial messaging and billing.

One question was, is it possible to spoof the so-called double opt in process. What each of the methods that Jennifer outlined have in common is that in security departments, the opt in for a carrier charge is a two factor authentication comprised of something that you know, and something that you have. And that's quite unique for our industry when compared to most other payment processes.

So that for example, when you swipe your credit card in store, it's one security factor-- single opt in, something you have. When you use a credit card online, it's generally considered one security factor, single opt-in of something you know.

In these billing methods, we have the strength of two factor authentication. Something you know, like entering your phone number or entering a keyword and texting it to a short code. And that's something you have, a message sent back to your cell phone and a way for you to confirm that actually the message was received at the handset.

In terms of ways to spoof that, nothing is invulnerable. And in our next panel, we'll discuss any missing holes that we, in our expertise, see.

There was another question about the transparency of the message logs, of the opt in records. Again the strength of this billing method is that it has handset authentication comprised of messages to a cell phone. Those message log are possessed by the consumer on their handset. They're possessed by the merchant on their side.

They're possessed by the aggregator, which has the complete set of exchange of messages. And they're also possessed by the carrier. So it's impossible for any one person in the chain to lie about it, if it ever goes into the discovery, for example, in litigation, because all of those records are always identical.

RUSSELL DEITCH: Let me follow up on that. Dealing with authentication, you said there are two parts-- what you know and what you have. In the first answer to the question, what you know is a phone number and what you have includes the pin that comes back.

Couldn't problems arise because, for example, the child could have the phone? And the pin comes back to the child who's too young to contract? Or a third party could have the phone. Because here we're talking about what you know and what you have. But it's not out of pocket type questions that only one person are unique to answer. And I know no methods perfect, but aren't there some potential holes with what you're describing.

ALLEN: Yes. I believe that there are potential holes. I guess, in theory, this method is superior to most other payment methods, which are single factor. In terms of a minor using a cell phone to make charges, this is sort of a larger phenomenon which is well accepted in our society in many aspects of cellular telephone use. Families use phones. Children use phones. And they incur charges when they do that. And this is not exactly an exception.

DUANE POZZA: Thanks a lot, Allen. Well, we are now out of time. It's time for lunch. This interesting discussion will go on. And I hope everyone comes back after lunch for the third panel because there's still lots to talk about. And thanks again to all our panelists. We really appreciate it.

RUSSELL DEITCH: Thank you very much.