— 41st Annual —
Global SYMPOSIUM ON RACING & GAMING 2014
Hosted by the University of Arizona Race Track Industry Program

WEDNESDAY, DECEMBER 10, 2014

ADW Issues — Funding and Fraud

MODERATOR:
Vin Narayanan, Editor-in-Chief, Casino City

SPEAKERS:
Micah Lloyd, Vice President of Operations and Business Development, Sportech
Christian Solomine, Vice President/General Manager-Gaming, PayNearMe, Inc.
Jerry Zimmerman, Vice President of Business Development and Compliance, UA Off-Track

Mr. Vin Narayanan: — whatever reason, and you're looking to digitize cash. Then sitting right next to me is Micah Lloyd. Micah is a director of digital operations and product development for Sportech. Everyone knows who Sportech is. Micah knows his way around ADW as well and is a real expert in everything to do with ADW. We have a fantastic panel.

I want to start off, and Jerry, let's start off with you. One of the things that's an issue in the industry is credit cards. In New Jersey in the iGaming space, for instance, we're seeing, what, 90 percent rejections of Visa in New Jersey in the iGaming space. In terms of the ADW world, what are we looking at in terms of credit card use and acceptance cuz that's the one major form of payment that a lot of customers like to use?

Mr. Jerry Zimmerman: From our perspective, and that's the Greyhound Channel, which very greyhound specific content in ADWs, we have looked at a number of different methodologies and looked at the money sense, we've also used credit cards too. The credit card industry funding has been incredibly painful over the years. We've seen a number of providers come in and come out of the industry, and sometimes we're sort of left short. Our customers are left short in trying to fund anyway you can. Is everybody aware of what's going on in New Jersey?

Audience Member: We can’t hear you.

Mr. Micah Lloyd: Is your mic on?

Mr. Vin Narayanan: We'll get back to you, Jerry. Christian, let’s start with you then. Let's start with, first of all, what is PayNearMe, and second of all, some war stories, maybe a little bit about some weird fraud things you've seen out there.

Mr. Christian Solomine: I wanna make sure mine’s on, are we all —

Technician: It’s coming. It’s coming.

Mr. Vin Narayanan: Apparently, I'm the only one you can hear, and that's really not how this is supposed to work.

[Laughter]

Mr. Christian Solomine: Back in the day.

Mr. Vin Narayanan: Back in the day.

[Laughter]

I'll give you an outline of how this is gonna work, and you'll know what you're looking forward to. Here's what we're going to be talking about today in no particular order. We're testing my ability to vamp here. We're gonna be taking a look at the different forms people use to fund ADW accounts, why they use those different forms, how effective they are. We're gonna look at the acceptance rates both from a transaction point of view of those different accounts. We're gonna take a look at what the adoption rate is for consumers.

We're gonna take a look at where along the conversion funnel do you get people to switch different payment processes, and how do you get them to adopt new payment processes? We're gonna have some fun, and this is where the war stories come in, about talking about fraud because with any form of e-commerce, with any form of — and ADW is essentially a form of e-commerce, you get people trying to rip you off, rip off the system. I was in Malta about a month ago at an iGaming conference. I was talking to 888 and Greentube, two of the big iGaming suppliers.

One of the forms of fraud they ran into was people were actually — there were firms that were collecting driver's licenses from various people who were paying them money, and they were using them to rent them out as identities for people to log on and register for iGaming accounts. Really bizarre. They couldn't figure out — so they're seeing weird anomalous behavior coming through, and their algorithms are flagging certain wagers and deposits and trying to play through bonuses and all this sort of stuff, and they're trying to figure out what's going on. Finally, they realized there was some fraudulent behavior. They thought they knew what was going on, but they couldn't figure out how to prove it.

Finally, what they ended up doing is they ended up sending letters to all of these depositors by postal mail saying, we suspended your account for thinking we've got fraudulent activity. They figured that because these were rented identities, no one would actually open and return the letter because the people living there, they've got — they're not gonna open the letter and actually respond. If they got a real person, the real person would actually open the letter, respond, and provide the necessary information to reactivate the account. Of the letters they sent out, they didn't get one response back. That's how they knew for certain that they were dealing with a fraud ring that was trying to abuse the bonus and abuse the system.

It was actually a really remarkable combination of steps when you think about it. They had their algorithms in place to look for fraud and look for security issues. They found it, but then they used a really old school technique to solve the issue, which was going to the post office and mailing a letter out. It was an absolutely fascinating discussion. I found that combination, actually, really intriguing, the new school technology flagging the abuse and the old school solution.

They talked about it. They said it took them a couple days to figure out what they were gonna do cuz no one's programmed to use the U.S. Postal Service or use any mail service to solve an online security issue or an online fraud issue, and that's what happened there. Are we good on the mics? Are we good? There we go. Let's start this at the beginning. Jerry, first let's start with you introducing who you are, what you do, and then we'll get into the credit card thing.

Mr. Jerry Zimmerman: Can you hear me okay now?

Mr. Vin Narayanan: There it is.

Mr. Jerry Zimmerman: Great. Thank you. I'm Jerry Zimmerman, vice president St. Petersburg Kennel Club, which owns Derby Lane, greyhound track in St. Petersburg, Florida, and also vice president of US Off-Track. We are an ADW that focuses primarily on Greyhound content, and then also we provide support services, call center services to other horse racing ADWs throughout the country. I think I was talking before about — and the question was on credit card specifically as a payment solution. When you look at credit cards as a payment solution, I think currently, the present gripe is with, I'd say, Visa-based credit cards more than anything.

That's because Mastercard, a couple of years ago, created a new merchant category code or how a credit card is processed so that it would be able to be processed when it was presented. Visa has not done that yet, so they're still processing under a generic gaming code, merchant category code, although there has been discussion that that's going to change. We've heard that for some time, that there was change coming. Supposedly, there's change coming next year. What this all means is that typically if a customer's trying to use, say, a Bank of America Visa credit card, it's not gonna go ahead and get through. It's gonna get rejected as a transaction.

What we saw, and Vin mentioned something about New Jersey, we're not in online gaming in New Jersey, but we talk to those people often. Similarly, what we heard them telling us was that they were being told the credit card acceptance rates were going up, but I think some of that has to do with the customers, which we've seen in our own ADW. Customers figure things out themselves. When a credit card's not working, they're not gonna keep presenting it. They'll figure out another way, whether it be ACH or some other method to go ahead and get funds into the account. Therefore, that will, to some degree, self-select for higher statistical rates of acceptance for it. Visa, I think, remains a problem. I think everybody would acknowledge that it is a credit card problem.

Mr. Vin Narayanan: Yeah. It's definitely a problem with credit cards. Just to back up a little bit, the way credit card transactions work is, for those of you that don't know, depending on the type of transaction you make, a merchant codes that transaction according to that number. Some credit cards, some banks automatically reject certain types of transactions. We work in an industry where some of our transactions automatically get rejected, and so that means that we have to find ways to get money into the system.

People don't necessarily want to have to go physically someplace to drop some money off. They like to be able to do it electronically. They like to be able to bet online. They like to be able to bet using their mobile devices. They like to be able to bet without going to the track. That's a big issue for the industry. Christian, what you guys do is you help solve some of those issues.

Mr. Christian Solomine: Yeah. Thanks. For those of you that don't know me, my name's Christian Solomine. I'm the vice president and general manager of PayNearMe's gaming business unit. We define gaming as ADW, iGaming, fantasy sports, social gaming. We're live with a number of ADW sites as well as iGaming in New Jersey for online poker and casino. We see some pretty interesting things. I got a couple of stories I wanted to tell you guys today. One is business-related. One's personal. I'll give you the business one first. In addition to fraud from a player side, we also see fraud from merchants from time to time, or just quirky things that happen.

About nine months ago, we originally created this cash transaction network for a whole bunch of other industries other than gaming, including apartments, apartment rent, car loans, utility bills. We got a call from a lady, and she was — she had a styling business that she did online, and she was selling hair weaves. We do our LexisNexis check and get some background information, set up the merchant. Everything's going fine. Over the course of the next two weeks, six more inquiries. We're saying, how many businesses are out there like this for hair weaves? Number two, how did they even find us as the supplier of choice for cash payments to pay for these things?

When we were digging into the other people that were inquiring about it, we found out they all lived in same neighborhood as the lady, and they were getting competitive wanting to start their own online businesses. We were getting all these inquiries not even from businesses, but just from other ladies that wanted to sell hair weave products online. That was a pretty funny one.

This one, I don't know if a lot of you guys use Craigslist, but I'm selling some wheels off an old Grand Cherokee online. This is a common one, but this was a personal one, but I thought I'd read it to you guys cuz I found it funny. I'm selling rims off a 2008 Grand Cherokee. I get a note from a guy named Jason Mayfield saying, "Hey, are your rims and tires still for sale?" I replied back, "Yes."

I'm gonna read to you what he says to me, and you guys can let me know what things jump right out at you in his response. He says, "Thanks for getting back to me. I will pay your asking price plus $50.00 to hold it for me. Please provide your full name and address so I can send your payment. I will be paying with cashier check, so it'll take two to three days to clear. As soon as the check clears, I will arrange for delivery with my assistant to collect from you."

Obviously, what jumps out at you? I'm gonna pay more. Nobody pays more on Craigslist. Cashier's check. If you're buying used tires for a Grand Cherokee, I really doubt your assistant's gonna arrange for transport of it. Me being a wise guy, this is my reply back. "If you want to hold them until you can pick up, I would prefer you do an ACH bank transfer. Please send me your social security number, date of birth, home address, your routing number and bank account number, and as soon as I initiate the transfer, I will arrange with your assistant for a pickup."

Mr. Vin Narayanan: No response?

Mr. Christian Solomine: No response yet. I'm still waiting.

Mr. Vin Narayanan: You didn't ask him to use PayNearMe?

Mr. Christian Solomine: No.

[Laughter]

Mr. Vin Narayanan: Really briefly before we get to Micah, explain how PayNearMe works.

Mr. Christian Solomine: Yeah. What we did was, we set up direct point of sale integrations with a number of key retailers throughout the United States. Right now, we're plugged into all the Family Dollar stores and the 7-11s. When you go to fund your account with online, whether you're playing ADW, you want to play World Series of Poker, whatever it may be, you have your options for ACH or credit card payments or pay with cash. When you click on pay with cash, we send a barcode right to your phone.

You take it to any one of those 15,000 locations, give them cash, and by the time you're back in your car, your account's funded. It's a good technology-based solution and an alternative to other funding mechanisms out there that either have higher fraud, people are worried about putting their information in online, or the 7995 coding for credit card rejections.

Mr. Vin Narayanan: Micah, you deal from a supplier standpoint?

Mr. Micah Lloyd: Right.

Mr. Vin Narayanan: Explain what you do and what sorts of methods of payment that you have to integrate into your system.

Mr. Micah Lloyd: Hello. I'm Micah Lloyd. I am the VP of operations and product development for the Sportech digital environment. I do use both of my colleagues' services and products. I can vouch for the integrity and funding, the lack of fraud use both of these services. We started doing ADW white label solution under e-bet technologies, which many of you know me from. Back in 2009, we launched several white label solutions in that summer, and we hit our first fraudster within 60 days.

Mr. Vin Narayanan: What were they doing?

Mr. Micah Lloyd: Credit card chargebacks. Most of the fraud that I do see are experiences related to the credit card industry specifically. This was an intentional fraud chargeback. This gentleman deposited funds, wagered the funds, had a grand time, did it a few times, and then within 60 days, we started receiving the chargeback notices. This was an eye-opening experience for us. We thought surely this was a mistake, reached out to this gentleman. He acknowledged that he had made those transactions and didn't feel like paying them anymore. We opened up litigation procedures, not realizing the futility of such actions.

To this day, this gentleman still pops up on our radar whenever we launch a new ADW deployment for our products, and we've got some 30-odd different deployments now. This guy manages to create an account and attempt to do it again. Now, the delight of having all these ADW solutions under our purview is that we do see all these different attempts across all the platforms to create accounts. A gentleman like this, this scumbag — this alleged scumbag, to keep popping up after five years shows some perseverance, but it shows the importance of the diligence of the operations team to keep up and monitor the new signups that are coming in. It's hard to do so without having all that information readily available. The majority of such transactions are — that I see are intentional chargebacks. These are people who truly are just trying to get free money. I would say a very low percentage of the numbers are ID theft, and I think we'll speak to that in a bit here.

Mr. Vin Narayanan: Yeah. We'll speak to that in a bit. Just to touch on something, you talked about the difficulty in terms of litigating this stuff.

Mr. Micah Lloyd: Yeah.

Mr. Vin Narayanan: What happens and doesn't happen in that process? Why is it so hard to make it happen?

Mr. Micah Lloyd: Ultimately, when it comes to the credit card processing, at least historically, the way we produced that was we would have all this proof that this is the individual who made the transactions. We have ID verification. We have fingerprinting of hardware devices. We know that it is him behind the computer doing these things. We have mapped it out with background checks that we can do with the signup aspects. Ultimately, when we present our case to the credit card company, their response is, "Was the card present?"

Invariably, in every case, these are all done online, and the process and procedures at that time and still to this day are — do not lend support of that. Ultimately, no, we don't have a physical signature. We don't have a card present. They hang their hat on that. These fraudsters understand that, and they get around that. It isn't a high percentage. I did some analysis in preparation for this discussion, and I pulled back approximately 10,000 signups over the past few years and referenced them against those that we have subsequently identified as undesirable. The percentage was slightly under two percent.

Now, it's hard to quantify that against how much money we have lost against these. It depends on how quickly we are able to identify that this person is an undesirable. Sometimes, it's a little more difficult than others. Sometimes, they're able to quickly ramp up and take advantage of a situation and get funded and wager it away or withdraw it on track. Sometimes, we're able to catch it before they even get a penny in, like the alleged scumbag who signs up for a new account. Nope. Closed. Other times, we see sometimes tens of thousands of dollars are lost.

Mr. Jerry Zimmerman: Then just to —

Mr. Vin Narayanan: Go ahead, Jerry.

Mr. Jerry Zimmerman: We have actually almost nil credit card chargeback. We practically don't get any. Now, we're conservative in how we approach our customers. As Micah pointed out, you have identity validation. You have all of those other tools. You have a tape recording of the customer placing the wager. In terms of the absurdity of it, when a customer says, "Oh, somebody stole my credit card."

Then you say, "Okay, they stole your credit card, and then they went ahead and used it to deposit funds in your account, and then they're gonna go ahead and get a check payable in your name out of the account, and that somehow was stolen?" With all that being said, we have very little. We see actually more challenge with the instant ACH aspect for fraud.

Mr. Vin Narayanan: What challenge does that present?

Mr. Jerry Zimmerman: In instant ACH, an operator will go ahead and provide the funding immediately. In other words, you have a customer that you've had some experience with. They have a good track record. You'll go ahead and say, okay, before the ACH clears, which will take up to, say, 72 hours, depending on which bank it's being originated from and which bank it's being received to, there's—there is a flow.

What we have encountered when we have done that from time to time where we'll see a little bit of chargebacks on that. Now, to Micah's point, it is typically either — it's not a fraudster, per se. It's typically the customer has reached really a tricky credit situation, right? They don't have the funds. They're bouncing a check that they feel it might be good, or it's gonna be good because they were gonna win situation.

Mr. Vin Narayanan: Christian, you see a different situation when you try to identify fraud coming through your system, right?

Mr. Christian Solomine: Ours is a little bit different. I'm not sure. By a show of hands, do you guys know the difference between open loop and closed loop products? Does everybody know that? I can talk through that. Open loop products are typically people — things you could buy where you could reload, and you can put cash on it, and you can pay for multiple things out.

Ours is a closed loop system. When we receive funding in, it's directly from an account we've set up with an operator and only tied to one specific person. Some of the things that we've done to prevent fraud or violation of regulations in different gaming jurisdictions is, we lock down all of the store locations that can accept funds in tied to the state where that type of gaming is legal. That's one of the things that we do. We also incorporate in velocity limits, so if somebody's —

Mr. Vin Narayanan: Explain what a velocity limit is.

Mr. Christian Solomine: For those of you that don't know, velocity limits are how much money you could put in on a day on a 30-day basis. It's an amount and it's a time basis. With our system, we'll put in — we'll allow up to $500.00 per day, and up to $10,000.00 rolling 30 days. The reasons we do this are, we can see if there's multiple funding sources coming in, so you're putting in more than would be outside of a norm. Somebody may be trying to do something with money laundering or otherwise. We also pass that data back to the operator so they could compare that. If somebody's using credit cards and ACH and maybe PayNearMe, they collectively can tally up all the different velocity levels that they're putting in different instruments and compare that too. We have that one-to-one.

Another thing with retail, because you actually have to be present versus credit cards, most of the retail locations also have cameras. When people are coming in, they many times have cameras outside, or they'll at least have them at the point of sale location. If you are depositing and trying to do nefarious things with it, you're also getting a record of your image tied to the specific state, tied to the specific address. There's other things that we incorporate on our end that can help aid either our sites or law enforcement with if there's any detected fraud down the line.

Mr. Micah Lloyd: Is there any chance that you can share that information automatically back through —

Mr. Christian Solomine: No. Not through the system. No. We don't have live video feeds. Not yet.

Mr. Vin Narayanan: This is interesting because you've got different types of fraud that are going on through the system. You're dealing with chargebacks. Then we've got a tricky financial situation where the money just might not be in the account for the ACH. Then Christian, you've got different sorts of checks coming in because yours is basically cash into the system. Those are three different things.

The most outrageous case of fraud that I've seen in the New Jersey iGaming scene is, there was a woman who gambled around 10 or $12,000.00 and lost all of it. She went through all the checks, went through the compliance checks, went through the identity verification checks and all that sort of stuff. She tried to claim her identification had been stolen. The police actually went out to investigate whether her identification had actually been stolen, and it hadn't been stolen.

In fact, she was — she tried to claim that she was someplace else when the bets were made, even though the geocompliance said she was in her house and her alibis didn't hold up. She tried to claim that someone had stolen her identity to buy a whole bunch of stuff. It turned out she's the one that bought all of that stuff. They went down through the whole thing. Now they're charging her with all sorts of fraud. It's a case where the local jurisdiction actually went in and investigated and said, "Yeah, no, you just wasted our time and resources, and now we're going after you."

Mr. Christian Solomine: Delightful.

Mr. Vin Narayanan: Yes. It's a different approach, but it points to the importance of having the proper controls in place to provide that evidence and information.

Mr. Micah Lloyd: We had some identification fraud issues that hit us in 2011 where we caught this surreptitiously by noticing similar signups that were happening in succession from the same geographic location in Louisiana, which in and of itself is not suspicious, but when it happens over and over and over and over again, it certainly — and we get these notifications that these are coming in, it draws attention and focus to it, and we start looking at it. It was very similar aspects to these signups. The e-mails were very generic and established the same way with a last name and a four-digit number at Yahoo.com. They're all very consistently how they're entered, all caps on the name.

There's little standard things that just jump out that if there were different people doing this, they would be entering data a little differently. Then the wagers. They would be depositing the large — $500.00 via credit card and subsequently make a single wager, a superfecta with very — a large amount of selections, hoping to hit a very big winner. When they didn't, they would just abandon the account and create a new one. Once we figured this, established this routine, this pattern, we were definitely watching and monitoring. This is happening across probably 10 or 12 different ADW deployments simultaneously, which we're observing. I'm not quite sure how many other ADWs that we don't have access to were being hit by this, which raises an interesting question for later.

As they're coming in, as we're noticing these, we subsequently start locking them down, waiting to see if these people would reach out to us, and they never do. This went on for two or three days and then stopped. Looking at the phone numbers, the e-mails were obviously fake, but the phone numbers were real. I personally contacted a few of the names of these accounts only to find out that these people did exist and had no idea who I was or why I was calling. I would gently suggest that they contact their credit card and check to see if there's been any fraudulent activity. I tried to escalate this to the police department, but I was not the victim.

Mr. Vin Narayanan: Jerry, Christian, Micah brings up something interesting in that one of the keys to dealing with security and dealing with fraud is having the proper controls in place, both on a transactional level, but also at the operator level. What are the sort of transactional level things that you have in place to help with that that will help operators?

Mr. Jerry Zimmerman: Do you want to go first?

Mr. Christian Solomine: Yeah. I'll go first. There's a couple things that we take a look at. One of them is geography, since every store is tied to a specific address. If you see somebody making deposits routinely in New Jersey, then all of a sudden, they show up in Tucson, they may live in New Jersey, might be here at the show and they're putting money in, but then the next day, they're in Michigan, and the next day, they're in Florida, there's things that you can tie that to and cross-correlate. That's one. A lot of the players also, because we're presenting mobile barcodes, will give their e-mail address or more likely, they're utilizing a cell phone number. They're gonna get this via SMS.

Now, many times, they may change e-mails, but it's much harder to change their cell phone number. You can also then cross-correlate your phone number tied to different accounts under different identities, and we can supply that information back. With any deployment we do with an operator, we do not set accept cash in without an approval. We will send a call back to the operator site to make sure that this person may — one, their account's in good standing. Two, they haven't exceeded velocity limits. Three, they're not in an OFAC. Four, they haven't signed up for any sort of mandatory gambling issue opt out. We'll do that as well. We want to make sure that when people are putting funds into the system, one, the site wants to accept it, and then and only then do we complete the transaction.

Mr. Jerry Zimmerman: I'd say from our perspective, we're doing a number of different things. First, from an operator's point of view, we've really beefed up compliance. We've spent really a ton of money, time, and energy in creating an absolute AML, anti-money laundering compliance team, where we have a designated compliance officer. We do independent reviews of it. We go ahead and have a formalized policy. There's training going on of the employees. From that perspective, everybody — and that's where FinCEN and the regulatory authorities are saying, you must do — you must first be trained to handle this stuff. We're doing that.

Then as Christian pointed out, there's a number of techniques and technical enhancements that you do, for instance, with ACH. With ACH, the first time we do an ACH with a customer, we'll do — and it's standard. We'll do either a microcredit or a split-credit transaction. In other words, we'll send them — and if you've ever been on PayPal, you might see this happen where they'll send you a few pennies, a few cents, and then you have to verify what you've received. Then they know, okay, this user has access to the account. We do that both in a microcredit check, or you can do it simply in their first transaction, splitting it into certain amounts, random amounts that will add up to the total. Then they have to validate the two amounts it was split into in order to, again, assure that they have access to that bank account.

Mr. Micah Lloyd: Operationally for the ADW world, we have morphed over the years and have grown a set of tools to help mitigate these type of issues of monitoring social security numbers and redundant entries of social security numbers across ADWs to find out if people are hopping around. Now, that does not in itself raise a flag that this person is nefarious, but it certainly draws focus that — something to look at. We look at additional activity throughout the day. If a customer makes multiple deposits of whatever sources, and there are no wagers between those deposits, it raises a very significant flag.

What is the purpose of making multiple deposits unless there's some attempt either to create a very large amount to make a very big wager, in which case I want to know cuz he's a bridge jumper or something, or there's other issues going on. If there are deposits and withdrawals at the same location with no wagers is the biggest flag I want to raise attention towards.

Mr. Vin Narayanan: We're looking at different funding types here. In terms of funding types, what's the general breakdown in usage that you're seeing?

Mr. Micah Lloyd: With all the different deployments, it depends. There are some brick and mortars that are very heavy into the ACH world where, thanks to velocity controls, it takes up some 50 percent of their deposits. In others, it's credit card. In others, it's purely cash at OTBs. There's no really across the board. There's far too many options, and it depends on each deployment.

Mr. Vin Narayanan: What about you, Jerry?

Mr. Jerry Zimmerman: We'll do everything, as I said before, from walking at the Bank of America person to PayNearMe to ACH and varying forms of that. It depends. It goes across. I would say we are more heavy on ACH than anything else.

Mr. Vin Narayanan: How do you get people into the various payment things?

Mr. Jerry Zimmerman For us, it's somewhat unique in the ADW business. Again, we have this Greyhound-based customer base. We have always, from day one, gone ahead and — as part of the way we do customer acquisition, the way that we manage our relationships is, we've absorbed that cost for funding. We're very sensitive to funding cost. What we experience then from the customer's perspective is, what's the easiest way, or what's the quickest way I can get money? That's what they're really concerned about.

At the end of the day, it's all about wanting to get money in so I can get money in the race or something. What we see with that is, anything that'll work, they'll go ahead and do. Whatever's working or not. We talked before about credit cards. If their credit card gets rejected, we'll immediately try to suggest, do you have other alternative methods? Typically, they're starting to get comfortable with us, so they're willing to go ahead and provide more of this data to do these other things.

Mr. Vin Narayanan: Comfort level's the key. One of the interesting things that's happening in New Jersey, Christian, is the fact that because credit card rejections are so high, when people go to deposit, PayNearMe becomes one of the top ones they recommend right away.

Mr. Christian Solomine: They first were trying to have credit cards at the top. When they first launched, there was a number of other banks that were supporting the Visa, and they were averaging between 30 and 40 percent. Once they started to see drop-offs, and then TD Bank pulling out of New Jersey dropped Visa acceptance rates around ten percent, they made adjustments to their funding pages. When people were going in and they were saying, "I want to use my credit card," they would pop up a window and say, "Are you sure? There's a very high percent chance this is going to be rejected," because they wanted to have a good player experience, so they were doing that. They were moving these different funding mechanisms in order cuz the way your eyes — you're reading top-down, typically, and they were pushing other ones up there.

Then in some cases, they would also use ours as a backup. If people said, "Hey, I've got a good credit score. I've got no issues. I still want to use my credit card," and they didn't understand it really had nothing to do that, and they still used it and they got rejected, then they'd use us as a backup mechanism. Then other people would just use, because they feel comfortable playing with cash, they would do it from day one. The sites have gotten smarter about dynamically optimizing based upon what is happening, success in the market, because after they've spent so much money to acquire these players, anywhere from $200.00 to $400.00, based upon all the marketing they're doing, the last thing they want to do is have them come and have a bad experience when they're trying to fund for the first time.

Mr. Micah Lloyd: Thanks to cash-based deposits, we actually have been able to recover some of the fraudulent funds that have been deposited previously. This alleged scumbag would — had previously took us for some funds, and yet opened up an account under one of our affiliates that's still under our operational name, deposited money via a cash-based solution, locked the account, seized the funds, apply it back towards the previous stolen money. He has no case.

Mr. Vin Narayanan:

[Laughter]

Has he learned his lesson yet? Has he learned his alleged lesson yet?

Mr. Micah Lloyd: It only happened once.

Mr. Christian Solomine: I think it's the same guy that's trying to buy my tires.

[Laughter]

Mr. Vin Narayanan: Yeah, it could be the same guy trying to buy your tires. It's funny cuz we're talking about the conversion funnel there. That's the iGaming lingo. Where in the conversion funnel do you put a new payment and try to get them to adopt it? Christian, what you were talking about is standard practice in the iGaming industry, which is, they actually try and funnel people to the preferred payment method, the one that they know is gonna work.

They know that Neteller's gonna work. Neteller's the first one listed. If you go to someplace else, they say, "Are you sure, cuz Neteller really works." It works out that way. A lot of them end up having deals with Neteller or Skrill or whatever their payment provider is. They try and funnel you in one direction or another. The customers actually get used to it. It's remarkable how quickly they get used to a different form. Neteller, for a long time in Europe, has been the primary way of funding online gaming accounts there. It's just de facto.

Mr. Jerry Zimmerman: Back years ago, if you're old enough, Neteller was supporting ADWs too, and they pulled that, as was PayPal.

Mr. Micah Lloyd: That's unfortunate.

Mr. Vin Narayanan: Yeah. Customers will get used to it, that's for sure. It is unfortunate they pulled out.

Mr. Micah Lloyd: It's tough.

Mr. Vin Narayanan: On the compliance front, what are the big compliance issues that you face?

Mr. Jerry Zimmerman: I think as I said, and you're seeing a ramp up because, I guess, of the advent of online gaming, but you're seeing — and also because of what's happened, I guess, with the gaming licensees out of Vegas and then Macau with these huge amounts of money moving back and forth with some of these VIP players. Clearly, there's been a push from the federal level to get a better handle on anti-money laundering with gaming. We've been doing that for some time, so fortunately, we're in sync with the requirements that are coming out. I think the — was it the action committee that works for gaming in general, they recently came out with their manifesto.

Mr. Vin Narayanan: The AGA.

Mr. Jerry Zimmerman: The AGA came out with their compliance, what you should be doing. Those were just the basic steps that FinCEN requires, what I identified before. All those things on the compliance side are things you need to be doing and thinking about for anti-money laundering because the authorities are now considering a gaming operation to have some of that risk. From a transactional or a product point of view, the biggest compliance side issue I've always seen has again been credit cards with the concept and notion of PCI or payment card industry compliance standards, which are set.

Even though they're set, it doesn't really prevent — we've seen all the cases that have occurred from Target on up with all these tremendous hacking cases and payment card frauds that have occurred, but yet, these standards are out there, and they're expensive and timely to try to comply with. Those, I think, would be the biggest challenge for any company, at least from what we've seen.

Mr. Vin Narayanan: Christian, how do you guys handle compliance?

Mr. Christian Solomine: You have all this external-facing stuff, but a lot of companies are getting more into this. We did this from day one, but we have internal compliance training. Every employee we bring on board, they have to go through that compliance training because one of the easiest backdoors into payment companies is going in through the employees and trying to fool them into certain — doing certain things without their knowledge on the back end. We make sure that everybody comes on board goes through full compliance training. We walk through the typical type of scams and fraud that we see in the industry so people can be extra alert when we get a lot — when we get inbound calls either from our consumers or from our sites or from our retail locations.

Mr. Vin Narayanan: You said typical fraud. I can't help, what is a typical fraud?

Mr. Christian Solomine: The common things you'll see are — I'm not saying any — specific to anybody's payment mechanism, but where people will want to buy a product. Maybe they're buying a $1,100.00 TV. They ship it to Mexico, and then they sell it for $0.80 on the dollar to effectively launder money. Those are typical use cases you see, so you got to be really careful when you're doing your checks on both your consumers and trusted merchants that they're not using these payment mechanisms for money laundering. A typical use case.

Some of the other things that we've seen in the industry, particularly with open loop products, the example I was giving you at breakfast where you get a phone call at 9:00 a.m. on a Sunday morning. You live in Colorado, and the Broncos game's about to come on. The person on the phone says, "I'm from Comcast. You're behind on your bill, but we need to get a payment or we're gonna turn off your cable." The person's freaking out. They want to watch the game. What do I do? My bank's closed. I can't use the other mechanisms. They'll say, "Hey, go down to your local store. Get an open loop product. Give us a call back. Give us the PIN code off of that. Then we'll keep your cable on."

The person goes down. They want to watch the game. They give them a number, an 800 number, and they call back and the person answers the phone. They're like, "Thank you for calling Comcast. How may I help you?" They give them the number, the code, and voilà, their cable doesn't get turned off. Needless to say, their cable was never gonna be able to be turned off, but the person thinks that. Only two days later when the regular office is back open, they find out that it was a scam. There's things like that happen all the time. Again, Craigslist type of things and otherwise. That's a common one as well where people are using open loop vehicles without protections to have people pay and then pull those funds out. Those vehicles are treated like cash, so the consumer's the one that loses out.

Mr. Micah Lloyd: We've actually been hit a few times with those open loop type scenarios where then the vendor would contact us because the victim would reach out to them after discovering that their Comcast was never gonna get turned off. They would reach the vendor. The vendor would see where those funds were deposited, contact us to see if there was any recovery left. Invariably, the answer is no. I've found that often, those were victims of ransomware issues on their computers. You hit the wrong site, and you get the FBI warning that you've got some nefarious stuff here. You are in trouble unless you pay $500.00, which happens to be the maximum amount of that open loop solution.

Mr. Vin Narayanan: You're seeing more of these open loop type vehicles being pulled off the market because of all the different fraud types that go on with them?

Mr. Christian Solomine: Ransomware's just nasty stuff.

Mr. Micah Lloyd: Good backups, people. Keep good backups.

Mr. Vin Narayanan: Yeah. Good backups, and don't pay the ransom.

Mr. Micah Lloyd: Just reformat.

Mr. Vin Narayanan: Yeah. Reformat the hard drive. Just ignore the whole ransom thing.

Mr. Micah Lloyd: Stop going to those websites.

Mr. Vin Narayanan: Yes.

[Laughter]

We won't say what websites those are. In terms of fraud prevention and utilization, what sort of detection services are being used?

Mr. Micah Lloyd: Diligence on our side. Monitoring. Active monitoring of transactional aspects, signup aspects, and just diligence. Our operations team — I don't want to use the word blacklist because my legal department gets all paranoid when I use that word — but blacklists that we don't —t hat don't leave our possession. There are people that are bad, and these are the things we have to filter up against. It's not automated. I can't share that with outside. I have so many different deployments that I can't just arbitrarily close down this one account, but I can send up a flag, this is a problem.

Mr. Christian Solomine: A lot of it's common sense too. Just asking a lot of questions when you're bringing on either — whether you get a consumer complaint or you get a merchant that wants to sell something. We had another one where they said, "We're operating an e-commerce site. We're selling books." Fine. No problem. We were seeing a lot of small transactions over and over and over again. We investigated in the site, and they had a parallel site tied to it. They were actually utilizing a purchase on the site to then convert to bitcoin. There's other things that they'll create a facade of what a business is, and then they're doing other things behind the scenes, just a cash to bitcoin-type conversion service, which is something that we don't support today.

Mr. Jerry Zimmerman: To tack on what Mike and Christian said, KYC. Know your customer. Know him really well. In the internal training, we also, as Micah pointed out, do the spot checks. We're looking. When we see something that looks suspicious, any type of activity in a customer's account, we'll go ahead and question it.

Mr. Vin Narayanan: Bitcoin. Does everyone know what bitcoin is? We have nobody.

Mr. Micah Lloyd: One person. One person over there. He knows what it is.

Mr. Vin Narayanan: Come on up here and tell us. We want people to know what bitcoin is. Bitcoin is — falls in the category of what's called a cryptocurrency. Essentially, it's an anonymous currency, so you can use bitcoin — the way it works is, you buy bitcoin. One bitcoin might be worth $100.00, and so you buy your $100.00, and you get the one bitcoin. The bitcoin is actually a string of numbers and hashtags. Then you use that as a purchase, and it's completely anonymous. When you buy something, if I wanted to place a bitcoin wager, I would place a — let's say it's a $100.00 wager. It's a $50.00 wager.

I'd take a half my bitcoin with the cryptocurrency, with all the little hashtag and security things, and I'd send to it an operator that would accept bitcoin. That would be the bet. They don't know where the money came from because they only know that hashtag thing. They have no idea what the source of the money is. They have no idea — there are no banks involved. There's none of that involved. Bitcoin has become a really popular cryptocurrency out there. I was wondering, and I didn't mention that we were gonna talk about this, but I figure I'd throw it open is, what do you guys think of bitcoin, the use of bitcoin, and whether that should become an acceptable form of payment for ADWs?

Mr. Jerry Zimmerman: I could tell you as a business operator, I would have concern—as I said before, and I don't want to deviate from that, any way a customer wants to get money in, we'll try to make that happen for them. We want the customer experience to be really good. My concern though as a business manager and looking at the businesses, I don't understand bitcoin. It was a good explanation. I still don't understand it.

I don't know what it would be worth. If I had it today, I don't know what it would be worth tomorrow. It would be very hard for me to build a business plan around it. If I were to deal in a bitcoin, if I had to, and we decided to do it, I would immediately hedge that transaction about a second later so I was sold out of it and knew exactly what I was getting so we were able to — we would do the transaction based on its merits as opposed to having this thing that the value might change.

Mr. Christian Solomine: There's a couple of small sites now operating, at least for poker, that are utilizing bitcoin, and they're doing exactly what Jerry just said. They're taking money in. They're immediately selling it back. They're putting it back in the online exchange so there's no risk of devaluation. There is a little transaction cost there, but they're doing exactly that rather than sitting on it. Other sites may just want to keep collecting and collecting and hope the rates go up, but if you guys have seen over the last 12 months, in terms of the volatility of bitcoin exchanges, it's — that's a much more risky proposition.

Mr. Vin Narayanan: There are actually bitcoin ATMs in Vegas now. I'm not kidding. If you go to — go down to Fremont Street, one of the casinos or a couple of the casinos down there have bitcoin ATMs where you've got your money in bitcoin, and you need to get them into dollars to play at the tables. You go to the bitcoin ATM, you put in your bitcoin security numbers, out comes cash that you can go gamble with. It is picking up steam as a currency, as a cryptocurrency. The online operators, the ones I've talked to, they're instantly putting it back into the system.

Mr. Christian Solomine: Also, you need some liquidity. You need enough people using bitcoin to play bitcoin games. There's a decent amount of people using bitcoin for various purposes, but not enough that it gets really interesting yet. I think once you build up that pool of people that are just using it for a whole bunch of different purposes — I think overstock.com now accepts it. I believe Dell. A couple other well-known sites, but you need a lot more. Then you'll be able to see games and other sorts of wagers accepting it.

Mr. Vin Narayanan: Germany actually declared bitcoin as legal tender so they could tax it.

Mr. Micah Lloyd: We haven't deployed it anywhere. We've barely looked into it. Understanding that funding is the key for our business to grow and our customers to use our services, it's inevitable, so I'm just gonna wait, Jerry, until your team gets it developed.

[Laughter]

Mr. Christian Solomine: I'll try to figure it all out.

Mr. Vin Narayanan: How hard is it to keep up with the various things people do to rip you off?

Mr. Micah Lloyd: We're constantly chasing after them. I've become very cynical in this — in that aspect. Unfortunately, I think the worst before I think the best. Perhaps someone has to do that.

Mr. Jerry Zimmerman: Yeah. I'd say I think in all of our roles, base of where we're coming from, we're looking at — we want the customer experience to be good. We want there to be a growth in revenue, but we have to — we're the ones that are forced to look at — it's like water running down a hill. They'll figure out a way to do something, and we always have to just be — you want to be vigilant on it without disturbing the customer experience.

Mr. Vin Narayanan: In any form of electronic commerce, electronic transaction, you've got to balance that customer experience with a friction point where they have to give up something that they don't necessarily want to give up, whether it's a social security number or whether it's a bank account number. How do you balance the two needs? You have the need to know who they are and where the money's coming from with the need to have a really smooth customer experience, especially when you have folks who are used to buying things off of Amazon with one click.

Mr. Micah Lloyd: It comes down to options. When it comes to the social security number, generally, that's not an option. We need to know who our customers are. Now, extending that information to the customer itself is an important message that has to be managed properly. When it comes to the funding aspect, there are options. We have as many options as we can in order to facilitate the funding mechanism. If they do not want to give credit card information or ACH, then we offer cash-based solutions. It is a matter of whatever the customer's comfort level is.

Mr. Christian Solomine: Different sites have different perspectives on this, but I've seen some registration processes where they don't ask for the social security number immediately because that's the one thing that drives people away. If you guys ever requested a credit report, they say, "Did you live on this street? What was your old zip code?" Those sorts of things. They'll ask all these questions, or they'll ask for the last four. The studies they've found, and it depends again on industry, and if this is allowed based upon Department of Gaming Enforcement or whatever it may be, if you do that, you get a much higher acceptance rate because it's not blasted right in their face right at the beginning of the registration process.

Mr. Vin Narayanan: Yeah. I moved recently, and so my landlord, for whatever reason, wanted me to pull my own credit report. I didn't understand why, but I really wanted to live in the place, so I said yes. I went to the various credit reporting agencies. They wanted me to take this test to prove my identity, and I failed two out of the three tests, which was really disturbing.

[Laughter]

Yeah. There's no missile coming right at this place. Don't worry. I failed two out of the three tests because the tests were just so fricking hard.

Mr. Jerry Zimmerman: You couldn't remember the street you lived on 16 years ago?

Mr. Vin Narayanan: No. They said, "Between 2004 and 2008, you bought furniture from IKEA." It's like, all right. They're like, "So what address were you living in when you bought the furniture from IKEA?" Between 2004 and 2008, I lived in four different places, and I probably bought furniture from IKEA at several points during those things. I had no idea.

Mr. Christian Solomine: It gets even worse than that. I've seen ones where they actually ask, "You did a loan on that, so you had a credit card. How much were you paying per month for that loan?" How would you know that? That's a little bit over the top.

Mr. Vin Narayanan: I had a friend who had bought two Hondas over the course of five years, one for himself, one for his wife, and they asked him a question about which car and which dealership he got it from. He's like, "Which one?" He had no idea. When you talk about friction points and trying to get the customer information, there is actually a lot of — there's a balancing act because you want to be able to verify them, but you also —

Mr. Micah Lloyd: Those soft fails are the bane of many of our customer issues or complaints, and there has to be a fallback. There has to be a manual method to validate and then take a photocopy of their ID and manually create this account outside the system because sometimes, people just aren't in the system as fully as we need them to be.

Mr. Vin Narayanan: The bane of your existence when it comes to ADW and security stuff.

Mr. Micah Lloyd: I'm gonna pass on that one for a moment. Bane of my existence.

Mr. Vin Narayanan: How about you, Christian?

Mr. Christian Solomine: It's not a bane. It's just making sure that anybody we work with fully understands how the technology works and building the proper authorizations back and forth. We get the systems talking properly, it grossly reduces any sort of attempted fraud. That's just getting them in place, making sure we're hitting the right database, and they're hitting the right database on our end so we can accept those transactions, but also have a good customer experience. You don't want to go to a 7-11 and have to wait four minutes for it to go through. We're working on that and making sure it's optimized so somebody can come in, they scan their code, they pay their cash, and they're out in 60 seconds is our goal.

Mr. Vin Narayanan: How much training of the folks at 7-11 do you have to do to make sure that those transactions go smoothly?

Mr. Christian Solomine: Tremendous. When we first started out, we only had one merchant. We had Greyhound, and we were doing all of their transactions. Nobody had ever seen the use of a barcode at retail, so we had to train an average of ten clerks at every store, and then a lot of different retraining on top of that. Now that we've built up a whole bunch of other industries and we're delivering millions of people to these different retail facilities, the clerks now see it regularly. In the beginning, it is a challenge to work with any sort of new payment source at a new retail chain.

Mr. Jerry Zimmerman: Yeah. I think Christian hits it on the head. For us as an operator, there's that balanced customer experience and the consistency of the vendors we're dealing with to keep things the same. You have to understand, that's sometimes difficult when technology keeps changing. I think that's really the biggest challenge that we see is keeping it consistent cuz, as you said, the customers get used to something. They like it. They're ready. They know what they want to do. They want to do something with you on your site. Then all of a sudden, something's changed, and that creates frustration for them.

Mr. Micah Lloyd: You have to understand that in my business model, my customer are often the tracks, not the consumer, so balancing their needs and their desires versus their customers' needs and desires is really an interesting lesson on my side. The onus is on them to make sure that their customers are happy, and when they're not, it still comes back to me. It always is a customer experience. I remember going and using the PayNearMe process for the first time as a test, a live test, and the guy at the 7-11 behind the counter was all excited because this was the first one he had ever done. The process was up and done, and we were out the door in 30 seconds. I literally got to the car, pulled it up to see, my account balance was already there. It was a beautiful process.

Mr. Vin Narayanan: The PayNearMe process is really good. It's a proven technology because if you go to other parts of the world, they use similar technology all the time. It's just that it's being implemented in the U.S. now, which makes a difference. When I traveled to Europe for years — I don't do it anymore, and I really wish I did cuz I just got socked with a major cell phone bill, but I used to carry just a tiny little terrible phone, but it worked for the purposes of texting and local calls. I'd pop in a local SIM.

I'd go to a convenience store and I would say, "I need to top up my SIM card." They're like, "How much do you want to put on there?" I'd say, "Give me ten pounds' worth. That should last me three or four days." They would give me a little code, and they'd print out a code on a little strip of paper. I'd punch the code into my phone, and I had a week's worth of calling and texting. That's been going on there for years. It's nice to actually have a similar sort of solution available in the States now where you can go to a 7-11 or just local retail and do that.

Mr. Micah Lloyd: Using Jerry's product, his product is deployed across many of the same ADWs that we are service providers for. It's interesting seeing the customers use that service to move the funds from one ADW to another. It happens, folks. Everyone's moving funds to wherever they get the best bang for their buck. How we've worked with you guys to make sure that those funds are on the up and up and everything works is a delightful experience.

Mr. Vin Narayanan: Just in terms of technological advances five years out, ten years out, what are we looking at? Where are we gonna be in terms of how we fund accounts and what sorts of fraud we're gonna be looking at, and what sort of identification that's gonna be needed to go into this?

Mr. Jerry Zimmerman: We had this conversation earlier today, and I'm not sure because I told you I thought that biometrics is gonna be an automatic. We saw Apple it out recently in their newest product. When I talk to people, people in the payments industry, they're very reluctant and concerned about giving up what they feel is information — it's just data, but biometric information.

I thought for sure that's where everything will end up, but now I'm not so sure because I think there's a contingent of consumer out there that doesn't want to share biometric data, although I think that it's all out there. If we've ever been fingerprinted for anything, it's out there, but people are still reluctant to get that mindset. Maybe with younger consumers as they come on, they may be more willing.

Mr. Vin Narayanan: They share everything on Facebook anyway.

Mr. Christian Solomine: One thing for sure is the move to smartphones. We have over 80 percent penetration of smartphones in the United States. It'll be over 95 percent in the next 18 months. People are now doing initial registrations on smartphones. That's gonna be one thing that continues, but then when you have that, you also can do geolocation. If somebody's saying, "I'm at home. I live at this address," you can now tie that in through your mobile app. That's another thing that you use to incorporate it right into your own registration process to validate.

Mr. Vin Narayanan: That's interesting because if you look at the big search engines like Yahoo and Google, they're actually going to a cell phone-based identification system. They want a cell phone associated with your account number.

Mr. Christian Solomine: Yeah. You combine that with wi-fi positioning, you get a really good feel that that person is where they say they are right when they are there.

Mr. Micah Lloyd: From our side, we don't want to deal with that. We want to deal with the wagering experience. We don't want to have to worry about the PCI compliance requirements. I'm looking to my partner, my vendor partners, to create the solution and allow me to integrate it seamlessly, iFrame, whatever and securely without having to worry about the security behind it.

Mr. Vin Narayanan: Yeah. To me, I'm looking at two things. One is facial recognition because every cell phone, every computer, every laptop, it has a camera attached to it. If you can turn the camera on and they could look at your face and they can match it to your ID, and they're gonna be able to do that and say, all right. You're definitely the person. It's gonna take three to five seconds to do. There are actually DOD, Department of Defense contractors out there that have created this technology. They've got it in for the — they've developed it for the military, and they've realized that other industries can use it and have a need for it.

They're actually in the process of beginning to go and say, all right, this is commercially viable technology now. Who's willing to use it? Who wants to use it? The more customers they get, actually, the cheaper the transaction cost becomes, and the transaction cost goes down to a point where operators are willing to use it. I think that's one place because a camera's just a really simple and easy solution. I think the other is gonna be using the cell phone as a primary identifier. I know I'm old enough to remember when you couldn't port your cell phone number. If you moved, you were getting a new phone number. If you switched cell phone companies, you were getting a new cell phone number.

I think now we live in an age where the only thing that — there are two things that stay constant about you in your life. Your social security number and your cell phone number. People loathe to give up their cell phone numbers, and so it becomes a good identifier. Then you get the location component into it. I think you're gonna — I think that's where things are gonna go from a security standpoint. From a funding standpoint, I think there are two interesting trends, and I'd like for both of you to comment on it.

One is that we're seeing, at least with millennials, fewer and fewer checking accounts started. They tend not to start checking accounts quite as frequently. If they do have checking accounts, it's just for their direct deposit paycheck to go, and then everything else is done via e-commerce of some sort, whether it's PayPal or something else. Is that a trend that we as an industry need to be on the lookout for?

Mr. Christian Solomine: It's that and credit cards. When I went to college, you could — they would be bombarding you with credit cards the day you show up as a freshman. You're 18 years old, credit card. They've give you $500.00 limit and you're good to go. Most credit cards today need a cosigner, so these kids that are going when they were normally getting hit up with a credit card at age 18, they need a cosigner. They're asking their parents. Parents are gonna say no. They end up skipping that whole process. Many times, they come out of college, and they don't have credit cards. That's another thing. It's a combination of both of those, and they are using alternatives.

Mr. Jerry Zimmerman: Yeah. For younger consumers, kids going to school now, what I see — my kids are out of school, but I see my neighbors and friends with kids in school. It's a closed loop system now. They're all incorporating. All the schools have their own closed loop card system that you can use everywhere. They actually encourage the students to do that as opposed to cash. They're using just a closed loop system, something specific to that university and to all the concessions around. Their parents can top it up and put money on it and so forth.

Mr. Vin Narayanan: Yeah. I think things like the Starbucks app, that works really well. You're using the app to pay, and you're getting loyalty programs on top of it. I can envision a scenario where as operators, you start offering the same sort of thing. You can fund it this app. You get the loyalty programs for using this app. You can make your wagers through this app. You get the whole thing flowing, and it becomes a different system. We've got time for questions? Yes, we do. We've got four minutes for questions. We've got two microphones here, so feel free to come forward. I think we've got one person.

Mr. Micah Lloyd: Step forward and give your social security number, date of birth.

Mr. Christian Solomine: Routing number.

Mr. Matt Hegarty: with Daily Racing Forum. Micah, you had mentioned a fraud scheme in which people that had stolen an identity tried to open an account and then bet a superfecta permutation and said that if they didn't hit, then they abandoned the account. Did you have any instance in which they did hit a superfecta, and then what did you do because when you look at it, they're using stolen money to defraud the people that are in the superfecta pool. Just want to see what the resolution would have been if there was one.

Mr. Micah Lloyd: They did hit one, and they attempted to do a bank wire, which we've checked the bank and realized the name that they'd given wasn't the name on the account. We seized the funds, waited for him to call and ask why they didn't get the bank wire. Didn't get a phone call, held onto those funds, and then pointed them towards the chargebacks that we subsequently received.

Mr. Matt Hegarty: I'm sorry. I probably should have stayed up there then. Who ended up then with the seized funds?

Mr. Micah Lloyd: Our company did, and they didn't account for all of the moneys that were stolen. We still —

Mr. Matt Hegarty: The payoff should have gone to the bettors in the superfects pool that won. Do you see what I'm saying? Was there any attempt to identify those people that should have received a higher payoff?

Mr. Micah Lloyd: I see your point.

Mr. Matt Hegarty: They'd stole the money, right? You knew it was stolen money you had betting in the pool?

Mr. Christian Solomine: The bet was valid. The bet was valid.

Mr. Micah Lloyd: Yeah. The bet was valid.

Mr. Vin Narayanan: That's a thorny philosophical question though.

Audience Member: — find a solution, but I'm wondering if this [inaudible].

Mr. Micah Lloyd: That's an interesting point. I don't have a ready answer for you.

Mr. Matt Hegarty: I appreciate it. I'm not trying to put you on the spot or anything.

Mr. Vin Narayanan: Go ahead and explain the philosophical question that was just raised, cuz it is interesting.

Mr. Micah Lloyd: Yes. The stolen funds increased the pool size, and it actually modified the payouts and what-not. There is a broad issue potentially across those actions. Where do you draw the line at a $2.00 stolen wager versus a $500.00 stolen wager? Obviously, someone's got to draw the line. It's not me.

Audience Member: On that same subject, wouldn't it have to work both ways? If the host track is expecting you to kickback that money that you've recovered, what about if you don't recover, and it ends up being a losing bet? It seems it should be reciprocal if it's — if they're gonna expect a refund, then they should be expected to absorb some of the loss if it's fraudulent.

Mr. Micah Lloyd: I appreciate that. I'll settle up with you later.

[Laughter]

Mr. Vin Narayanan: Any other questions or topics we didn't touch on that you want us to talk about? At the back. Yes?

Mr. Éamonn Toland: Hi. I work with Paddy Power. I just wondered whether the panel was using device IDs extensively to prevent fraud. In Europe, we would use Iovation. They capture data on individual devices, individual iPhones, and that data is pooled. If somebody has experienced a fraud, whether it's a sports betting company or otherwise, that becomes a red flag when that same device ID is used to open up an account. We know that that smartphone has been associated with a fraud in the past. Are you guys doing anything similar in the U.S.?

Mr. Jerry Zimmerman: I will say that, again, we have — our fraud issues are not —I t's not usually fraud as Micah started off this panel with. It's usually because of a credit — really, it's a credit underwriting issue for that consumer because we've already done a lot of KYC work on them. We do have access to being able to do that. We have done it when there's been some questions and suspicious activity. I don't know that we've incorporated it as extensively as has been done elsewhere.

Mr. Micah Lloyd: We have desires to actually do — bring that into the fold. Part of our fingerprint aspect. Do you raise a flag that this is a similar transaction to a previously identified issue is a high desired item.

Audience Member: Thank you.

Mr. Vin Narayanan: Anyone else? I think we hit the number on the nose. I'd like to thank the panel for a great discussion. This was fantastic. I appreciate it. We hope you learned a lot, and if you have any other questions, feel free to come up or grab them in the back of the room.

Mr. Micah Lloyd: We have to de-mic.

Mr. Vin Narayanan: You have to de-mic now.