FTC FinTech Series: Crowdfunding & Peer to Peer Payments
October 26, 2016
Segment 1
Transcript

EVAN ZULLOW: Well, good afternoon, everyone. My name is Evan Zullow, and I'm an attorney in the FTC's Division of Financial Practices, which is in its Bureau of Consumer Protection. Welcome to all of you, and thank you for coming to our FinTech Forum on Crowdfunding and Peer-to-Peer Payment Systems.

Before we begin our substantive program and Commissioner McSweeny's remarks, I just wanted to walk through some administrative details that we're required to convey. First of those is, if you could, please silence your mobile phones or other electronic devices. If you need to use them during the forum, just try to be cognizant of others in the auditorium.

Please be aware that, if you leave the building for any reason during the forum, you'll have to go back through security screening, which could cause some delays for you. So particularly, if you're a panelist, please try to account for that so we're moving ahead on schedule. Additionally, most of you received a lanyard with a plastic FTC event security badge. We do reuse these for other events, so if you could, before you leave, just hand those in to the event staff.

Additionally, if there's an emergency that requires you to leave the conference center, but remain in the building, please follow the instructions that will be provided over the PA system. If there's an emergency that requires you to leave the building, an alarm will sound. If that happens, please leave the building in an orderly manner through the main 7th Street exit. After leaving the building, turn left and proceed down 7th Street across E Street to the FTC emergency assembly area. Please remain there until instructed to return to the building.

Also, as always, if you notice any suspicious activity, please alert building security. And please be advised that this event may be photographed. It is being webcast and recorded. So by participating today, you are agreeing that your image, and anything that you say or submit, may be posted indefinitely at ftc.gov, or one of the Commission's publicly available social media sites.

Restrooms are located in the hallway just outside the conference room. And during our panel discussions today, if you're interested in submitting a question, please fill out one of the question cards located at the table just outside the first set of doors in the back. Please just wave the question card over your head, and we'll have someone come and collect it and deliver it to the moderators.

And that's all for administrative details, so we can start our program. And we're very excited to have the pleasure of introducing Commissioner McSweeny. Thank you.

[APPLAUSE]

TERRELL MCSWEENY: Good afternoon, everybody. Thank you so much for being here at our second FTC FinTech workshop. We are delighted to have you here today. And a special welcome to the folks that are joining us on the internet through our streaming video as well.

We are focusing today on emerging financial technologies and their impacts on consumers and businesses. Innovations in financial technologies, which we know collectively as FinTech, have the potential to transform the way consumers engage in their most fundamental day to day financial transactions, including how they share, spend, and raise money. For many consumers and small businesses, such technologies can represent a life-changing opportunity to gain access to important financial services. These technologies also offer us all the ability to complete transactions and manage our basic finances more quickly and conveniently.

Last June, the FTC opened this FinTech series with a forum focused on marketplace lending. Today, we turn our attention to two other important growing financial technologies, peer-to-peer payment systems and crowdfunding.

Peer-to-peer payment platforms have become hugely popular in today's marketplace, particularly among younger consumers. With a few taps of a smartphone, these platforms allow consumers to exchange funds with one another directly. For example, splitting a dinner check, or, in my case, paying a babysitter, without the need to hand one another cash, or to write or mail a check. Such platforms can make transferring money faster and more convenient for consumers than other traditional options. So it should be no surprise that, according to a 2015 survey, 46% of consumers report that they have used a mobile app to make a peer-to-peer payment, and 27% of consumers report that they do so at least monthly.

Given the broad and growing use of these platforms, it's important to ask what protections they have for consumers. For example, how do these platforms ensure that consumers' funds get to their intended recipients, and that they are not diverted to potential scams? If consumers do experience a problem with a payment, or wish to dispute a charge, what's their recourse? To what extent are peer-to-peer platforms protecting consumers' privacy and data security? And how do all of these protections compare to those provided by financial institutions, and other entities, that have traditionally overseen fund transfers and payments in the past?

The FTC previously explored similar questions in our 2012 workshop on the mobile payment industry, and in our subsequent 2013 staff report on mobile payments. During our first panel today, we will examine these issues more closely in the context of peer-to-peer payments.

Following that discussion, we will, then, take a look at crowdfunding. The basic concept of crowdfunding is nothing new. For many years, some entrepreneurs and fundraisers have sought small contributions from a large number of people to finance their projects or causes. However, the emergence of online platforms has greatly expanded the use of crowdfunding as a mechanism for seeking charitable donations, financing the creation of a new project or a venture, and even selling securities. In fact, the Smithsonian has even got in on the action using crowdfunding platforms to fund preservation projects, such as Dorothy's ruby slippers or Neil Armstrong's spacesuit.

According to Mass Solution, in 2015 alone, crowdfunding sites raised more than an estimated $8 billion globally. Consumers, in turn, can use online crowdfunding platforms as a way to more easily find and contribute to the project or causes they are passionate about. In some cases, by funding a project, consumers can get an early prototype of a product, or even some other small reward.

However, as the use of crowdfunding continues to expand and evolve, it has also attracted some scams. For example, last year, the Federal Trade Commission brought its first ever law enforcement action against a fraudulent crowdfunding campaign. In that case, called Forking Path, we alleged that the defendant claimed he was raising money from consumers to produce a board game, but instead he used most of the funds for personal expenses. So today, in our second panel, we're going to dig further into both the significant promise and the associated risks with crowdfunding.

And as a lead into that panel, the Federal Trade Commission's Office of Technology Research and Investigation will provide presentations surveying the largest crowdfunding platforms, including the information they provide to consumers, and collect from campaigns. As we recognize the significant potential benefits of FinTech, we all must work together to ensure that we protect consumers from risks or unlawful activity arising from the changing landscape. The Federal Trade Commission is committed to doing so through both law enforcement actions, outreach, and educational efforts like today's forum.

So I'm looking forward to today's discussions, and I want to thank the team that has worked so hard to put this event together, including our Federal Trade Commission staff-- Evan Zullow, Elizabeth Kwok, Patrick Eagan-Van Meter, Duane Pozza, Malini Mithal, Stephanie Cox, and Jessica Skretch . I'd also like to thank all of our panelists who've taken time out of their busy schedules to be here today, and I look forward to a terrific discussion of these important issues. Thank you very much.

[APPLAUSE]

DUANE POZZA: Can you hear me? Great. OK. Good afternoon, I'm Duane Pozza. I'm an assistant director in the Division of Financial Practices.

PATRICK EAGAN-VAN METER: And I'm Patrick Eagan-Van Meter, a program specialist in the Division of Financial Practices.

DUANE POZZA: So we'll be moderating today's panel on peer-to-peer payments. We have a great panel here today to talk about this topic-- The Emergence, the Path Ahead, and the Implications for Consumers of Peer-to-Peer Payment Systems.

I'm going to give a short introduction of each of our panelists, then kick off the discussion with some questions and dive right in. I expect that each of our panelists will talk a little bit more about their background as they're going through and giving their perspective on peer-to-peer payments as we go along. Actually, Patrick is going to do a quick introduction of each of our panelists here.

PATRICK EAGAN-VAN METER: All right, to my immediate left, we have Jo Ann Barefoot, Senior Fellow at Harvard University's Center for Business & Government at the John F. Kennedy School of Government. And she's also the CEO of Barefoot Innovation Group.

Down at the end, Matt Van Buskirk is the Co-Founder and CEO of Hummingbird Fintech, and was previously the Director of Compliance at Circle.com.

Beth Chun is an Assistant Attorney General for Special Projects in the Consumer Protection Division of the Office of the Texas Attorney General.

Brian Peters is the Executive Director of Financial Innovation Now, an alliance of a leading technology companies-- Amazon, Apple, Google, Intuit, and PayPal.

Christina Tetrault is a Staff Attorney on Consumer Union's Financial Services Program team, specializing in banking, payments, and financial technology.

DUANE POZZA: So we have lots to talk about today. We're going to start by talking about some background and trends on peer-to-peer payments, and then delve a bit more into the potential benefits, the potential consumer protection issues, the legal landscape, and best practices going forward.

So my first question, I want to start off by talking briefly about the general state of the marketplace for peer-to-peer payments, and any important trends in where it's headed. In particular, there are many available standalone peer-to-peer payment apps right now. Is that the future, or will we see more consolidation and more of these services being offered by larger platforms? And I'd like to pose that question to all of our panelists, but first to Jo Ann.

JO ANN BAREFOOT: So thank you. And I want to commend the FTC for putting this program together. It's such an important topic.

So the first thing to think about with FinTech is predictions are dangerous and nobody knows where all of this is going to go, which is one of the reasons the regulatory challenges are so tremendous. But I think we'll see the emergence of both. I think we'll see both sectors really growing rapidly, and the marketplace will be sorting out what is likely to happen.

I do think we are likely to see a great deal of activity from the big tech firms that have such robust relationships with the consumer, have so much data on the consumer, understands us so well. Some of them are sort of beloved almost by consumers. Whether they deserve it or not is something people like to debate. But I think that we'll see a surge in those kinds of services. But I think the standalone small innovators are going to be very powerful also.

DUANE POZZA: I'll ask Matt the same question, too, coming from the small innovator perspective.

MATT VAN BUSKIRK: So Circle's perspective on this-- and I should say, since I'm no longer with Circle, I cannot officially speak for them in any means, so take this as my personal opinion-

- the perspective that we had when we were there, and that the co-founders of the company articulate very often, was that there had been a lot of development in sort of closed network payment systems. And you guys may have heard of Circle, as the pilot product there was a bitcoin-centric product connecting to the blockchain. Ever since then, it's been a little bit more following a traditional closed network model, with currency payments within-- domestically in the US, and then in Europe-- currencies that people would know and recognize. But they're always keeping that sort of interoperable open network concept in the background there.

So as these technologies develop, my personal stance on it is you're going to see a plethora of closed network systems, like Snapchat, Facebook, all these other companies coming out with their own payment structures. But it's much more powerful if all these platforms can talk to each other. So I think you'll get a hybrid model coming out of it, where you'll have closed networks for the systems you use most frequently, but they'll have some means of communicating with each other and settling, which will hopefully not be the ACH network, or anything like that.

DUANE POZZA: And I want to ask Brian, and also throw in another question. If these services are going to be provided by larger incumbent players, are they likely to be provided by banks or technology companies, or both?

BRIAN PETERS: Well, let me first say thanks to the FTC. We see the Commission as a partner in helping to raise the level of trust in the marketplace. We believe the FTC has a strong role in a lot of these financial regulatory discussions. So we're happy to be here. Thanks, guys.

I am speaking on behalf of Financial Innovation Now. I may use specific examples from the companies I represent, or others, but I don't speak on behalf of any one individual company. I just speak on behalf of Financial Innovation Now.

So I would say that I definitely agree with Jo Ann, that it is both, that you see payments being suffused into the media and communication channels that consumers have already flocked to, or flocking to, or may flock to next year. You also see standalone apps. And I think we're going to continue to see that for a while. So we'll have that diversity.

And I think, to dovetail with what Matt was saying, we see this generally as more of a disruptive pattern. While I think one of the-- I'd say dominant -- or the larger peer-to-peer services comes from one of the large US banks, most of the key features of peer-to-peer payments is coming from new entrants. So there's a wide variety of companies. I'm just going to list off a couple of them, but Circle, Dwolla, Google Wallet, Facebook Messenger, PayPal, Popmoney, Snapcash, Square Cash, Venmo.

And I think it's our perspective that those services are really changing the game of what money means to consumers. They are raising significantly our expectations of how our money should move, and how we should be able to move it. And I'd just say that some of the hallmarks of those expectations are that it is secure, that it's fast, that it's accessible, that they have control over it, that it is affordable, if not free, and, importantly, it's also, sometimes, social.

So things are early days here, right? Like, this is a nascent industry. You know, Venmo is doing, I think, around $4 billion per quarter about now. But that pales in comparison to about the trillion that sloshes around in the banking system in consumer payments. So that's still where we are. It's nascent, growing, and exciting.

DUANE POZZA: Christina, did you want to add to that?

CHRISTINA TETREAULT: Sure, I just wanted to add I think that we'll see a lot of changes as we move towards real time payments. So folks may or may not be aware, the Federal Reserve has convened a number of different segments of the marketplace, including consumer groups, and I'm a member of the task force that's looking to bring real time payments to the United States. And I think, as the efforts move forward within the task force, and outside of the task force, I think there will be a tremendous amount of change that comes to payments, but particularly to peer-to-peer. And some of the issues that we'll talk about today may be resolved and dissipate, and others may surface. So I think it's a really exciting time, and I anticipate a great deal of change in the next couple years.

DUANE POZZA: And Beth?

BETH CHUN: Thanks. To follow up with what Brian and Christina were just saying. But first, to begin, to introduce myself, I always need to make sure to say that the information that I am providing to you today should be considered general information, and should not be considered legal advice. And the opinions expressed by myself today are my own, and do not represent the Office of the Attorney General of Texas.

So I think that what Brian was mentioning is important, the fact that there are all these different iterations of peer-to-peer payments that are popping up, including Venmo. The Office of the Attorney General of Texas did obtain a settlement with PayPal regarding their Venmo app in May of this year. And I think that brings up an interesting point, that the social network aspect of some of these apps may not always be something that consumers are expecting.

And so, to the extent that those pop up, and these sort of peer-to-peer payment systems, it's important that consumers are made aware of the differences between these new technologies, and what they might be expecting with traditional financial institutions, such as banks and credit cards. So I think that it's great that there are all these innovations, and all of these new technologies. But just making sure that companies are keeping up with their disclosures to people about how those technologies differ than what they might be expecting, and then making sure the consumers themselves are also paying attention to those disclosures and understanding those differences.

DUANE POZZA: So a couple people have brought up the social, or the social media, aspect of it, and I want to get back to that later on in the panel. But I want to turn and talk a little bit about the potential benefits of these products.

PATRICK EAGAN-VAN METER: In her opening remarks, Commissioner McSweeny mentioned the potential benefits peer-to-peer payment services can provide to consumers. What do you think some of those benefits are? And we could start with Jo Ann.

JO ANN BAREFOOT: I'm glad you asked. I think the most important thing to think about in payments innovation of all kinds, and FinTech innovation overall, is to remember that there is an opportunity here to unlock incredible benefits to consumers, beyond what we've ever had before, in terms of affordability, access, consumer protection, empowering of consumers. And some of that is beyond the scope of our peer-to-peer conversation, but we should never lose sight of it, because the upside opportunity is historic. And there is a lot of downside risk at the same time. And as regulators, and I'm a former regulator myself, we have a tendency to go straight to the risk, and it's harder to think about the opportunity.

The benefits in this space include, keying off of what Matt said, that, if you're moving money on the internet, then basically you're doing for money and value what we have done for information. You're making it reachable for everyone, and instant for everyone, and almost free, apart from what it takes to put together the compliance programs and the operational things that have to be in the background. And that is transformational for people who need to move money around, whether it's remittances, or whether it's wiring funds, or whether it's just going through the payment system.

And I'll just call out one area, which is, if we had real time payments, which this is helping us push toward, the consumer would have far fewer problems that come from the lag in the payment system. An awful lot of the reliance that we have today for people who are using the expensive cash based services are it's driven by the fact that they can't know, other than with cash, exactly when something is going to be credited. If you write a check, or even if you use an electronic payment in most forms, you really aren't absolutely sure when the money is going to be in your account, when it's going to go into your account.

Sometimes it's being described as like having a whole 'nother job to go cash your check and go around and pay your bills, and that is partly a timing problem, a precision timing problem for people who don't have any cushion. If we suddenly have the ability to be sure that, if you make a payment, it's there, and it didn't cost you anything to have it happen, then a lot of the problems we have with overdrafts, payday lending, and so on, would go away. So that's just one huge area.

Now, instant payments raises all kinds of other problems to, which I'm sure people will talk about. And the regulators need to be thinking about those. But the benefit is enormous.

PATRICK EAGAN-VAN METER: Matt, do you have anything to add on that?

MATT VAN BUSKIRK: Just to push, or further expound, on the cost factor of this, too. Both speed and cost. Historically, if people need to move money quickly, it can be done, but it's very expensive. It's available to higher income individuals who have maybe personal bankers or businesses that need to wire money. But if you need to send money somewhere quickly, particularly across borders, as a moderate to low income person, it's a completely different

challenge. And you may be paying fees that are disproportionately outsized compared to the actual transaction.

One example I like to use is my sister, who, until about a year ago, was studying abroad in London. And she had to go through a massive amount of rigmarole to get money from family in the United States into her account in a British bank. Not to continue to promote Circle too excessively, but if we had been live at that time, she could have had money in her account immediately for approximately 50 basis points, or whatever the exchange rate modification was at that time. And there are other services, like TransferWise and others, that are providing similar capabilities at a fraction of the cost of the traditional payment system.

So just to reinforce it, the upside is huge. There are use cases we've not even thought of. I am really interested in the concept of micro-payments as well. Very intrigued to see where they're going to go. And obviously, my job at Circle was very focused on the downside and mitigating that risk, so I'm sure we're going to get into that a little bit later.

PATRICK EAGAN-VAN METER: And Brian, in your answer could you also talk about the benefits, in terms of expanding financial access to underserved consumer populations?

BRIAN PETERS: That's what I was going to do.

PATRICK EAGAN-VAN METER: All right.

BRIAN PETERS: No. Jo Ann and Matt both said it right. I think the hallmark consumer benefits that I mentioned before as consumer expectations really do have, I think, some of the most potential for the underserved. The underbanked and the unbanked together account for 26%, 27% of the country here in the United States.

When Jo Ann was talking about speed, speed is critical when it comes to households who are living paycheck to paycheck, or if they are financially stressed for whatever reason. Her point was spot on. If they don't know that the money will be there and be available when they need it to be, they're more likely to turn to alternative financial services, which are, as we know, check cashers that charge 1% to 5% to get access to your money, just to turn it into cash, or payday loans, or title loans, or other kind of very difficult spirals to even poorer financial health.

So to the extent that this can be a model, and that it can be even taken advantage of by the underserved, and it is a consumer expectation that everybody has, because I think we all face challenges with some of the friction in the financial system. Technology companies like the ones I represent, that's their whole focus, is they're always about moving things as quickly as they can, and removing friction and pain points from people's lives. And in the financial system, there are a lot of pain points. If you can remove those, those, I think, have a disproportionate negative impact on the underserved.

Just to put a finer point on it, the average unbanked household gets by on $22,000 a year. Their use of alternative financial services usually means that they're spending $1,000 of that $22,000

just to access their own money. If we can avoid that, even in some portion, that would be a huge advantage.

DUANE POZZA: Do we have a sense of the current demographic of the user base of these products. I mean, the sort of stereotype is it's a bunch of millennials splitting the bill at dinner, or whatever. And that certainly is a use case, but what do we know about that the rest of the current population of users?

BRIAN PETERS: I'll go first. So, yes, the perception is that it is millennials, and the research actually backs that up. Javelin has some research out there, and they showed that, over a 12 month period that they did an analysis of, millennials average 11 transactions over one year. But interestingly, those age 45 to 54 made four transactions over the same period, and 65 and older did three. So while it follows the age line in kind of a typical trend, the important point is that people across all age groups are actually using it.

And if you think about, at least in the strict peer-to-peer context, when you think of some of the more popular services, and you see the emojis, it looks like most of it is for going out at night and entertainment expenses. But the reality is, behind the scenes, a lot of people have chosen not to share what their payments may comprise. And so Javelin also shows that the most popular P2P payment purpose is for gifts. It's 39%. Bill payment is 38%, followed by entertainment expenses at 29%.

So you think about family-- it's easy to talk about friends trading money back and forth, but family, you think about taking care of your grandchildren, or taking care of your parents. We do a lot of exchanging of value within families across borders. And this really represents a great opportunity for that. So it's a little bit more interesting than I think you would give just millennials credit for.

JO ANN BAREFOOT: I just wanted to say that most FinTech innovation does aim first at millennials. Not all of it, but a lot of it does, because they're the early adopters. If you're a startup, and you're trying to find a market, and you've got a certain amount of capital and you're going to run out of it, you're not going to start with a group that doesn't use mobile based technology very much. But we shouldn't let that fact get us into the thought that somehow these things are just a niche product. They're starting there. Most of these companies plan to change the whole way the whole system works.

If I could tell a quick story. I don't want to take up too much time. But on this point, I'm on the board of the Center for Financial Services Innovation. And we have a exercise there we call Fin-X. And they could do it for the FTC, if you're interested. They help people go out into the city and try to transact some financial tasks the way you might do if you don't have a good banking relationship, as I'm fortunate enough to have.

So we had a board meeting a few weeks ago, and they sent us out into a Chicago neighborhood for 90 minutes to do tasks, like cashing a personal check, cashing a paycheck, buying a prepaid card, spending money on the prepaid card, reloading it, sending a money order. I can't remember all of it. And we ran all over the town. We had a lot of fails in my group. We were treated pretty

well, which some of the groups were not. But there were a lot of things where we went to a place, and they just said, we can't do that for you. It was very expensive to do it.

So it was very eye opening about how hard it is if you don't have a strong financial underpinning to function. But the other thing I took away from it is, I'm a Circle customer, and if the system worked the way Circle does, I could have stayed at home and done every single one of those things in five minutes. The whole thing. You know, that's where we should get to for everyone. That it's easy and it's fast and it's cheap.

PATRICK EAGAN-VAN METER: Matt, do you want to follow up on that, with that great lead?

MATT VAN BUSKIRK: Yeah, well I wanted to make one quick point, too, that obviously here we're focused on what it looks like in the United States. But the peer-to-peer payments ecosystems internationally are very different, and are targeting very different types of consumers as well.

Thinking about, beyond the millennial use cases, obviously M-Pesa has made a lot of news in Africa for getting financial services into places where they have not existed previously. And then, China really has put peer-to-peer payments on the map. They're the leaders in terms of market penetration and usage, through things like WeChat Pay. And the social gifting, the red envelope structure that they have there, I mean, huge amounts of money are moving around for gifts of various kinds.

So I think in the United States and in Europe, there is definitely a millennial focus. Circle certainly is catering specifically to them. There are a number of other companies that are targeting college students, because you can get some nice network effects, if you can penetrate certain universities, similar to what Facebook did. But we should keep the international differences in mind as well.

DUANE POZZA: So I want to talk a little bit about the legal framework. Obviously, there are many laws that apply in this space, too numerous to discuss all of them in detail. But you know the laws that apply to financial transactions generally. And we're focused here on the consumer protection side of it, as opposed to something like money laundering.

So Christina, I wanted to turn this over you. What do you see as the key consumer protection laws, and the key consumer protection issues, in this space?

CHRISTINA TETREAULT: So I would say the first thing is that usually the consumer protections that apply follow the underlying funding mechanism. And because those vary so much from across offerings-- so not all peer-to-peer services allow you to fund the services similarly. It's important to keep that distinction in mind.

So some of the bank peer-to-peer services are relying on ACH's from bank account basically to bank account. Some of the intermediary services allow the use of debit or credit cards. And then some, including bank offerings, allow the use of a prepaid card. So you're looking at these different sets of legal protections, depending on which that is. So if you're using a credit card, for

example, you have the most robust consumer protections. You have a chargeback right and some other things.

So that's sort of the big picture. But then again, it's really the devil's in the details. So when you dig into some of the consumer disclosures for the different offerings, you find various levels of help and assistance for resolving errors, for resolving fraud. We haven't seen any service that says you're on the hook for fraud, and I don't want to create that illusion, because that would be false. But there are varying levels of help that are offered.

So some of the terms and conditions explicitly say, you know what, you need to reach out to your bank. You need to reach out to your debit card provider. And others say, to the extent that we can, we will help you, and you need to do x, y, and z. And so painting with a broad brush is very difficult in this instance.

I will say that also underscores what I think is the most important thing to understand about the way these systems work, is these hugely complex liability chains. So your actual phone manufacturer is sometimes mentioned as a party to some of these agreements. Your telecom provider, if you're using an app. Your bank. Again, your card issuer, depending on what the financial service is. And then you've got this intermediary, the service itself, in some instances. In some instances, that might actually be your bank, so that's not necessarily comparable.

And then you have the people you're transacting with. So there are some aspects of transactions that the consumer can end up on the hook because they sent money to the wrong person in error, and that's one example where you're just out of the money if you, say, typed in the wrong phone number. But you can also be on the hook if you receive money from a friend who later reverses that transaction, and there can be a huge time gap before the transaction is actually final, even though you've gotten a notice and you think the funds are there. And by one example that I'm going to use is 60 days. So you can be on the hook if you spend money that you end up basically not having.

And so the legal framework is actually pretty complicated, and I think very hard for consumers to understand, when it's not necessarily clear that the protections would vary so much.

DUANE POZZA: I also want to ask Beth, to get the state perspective.

BETH CHUN: Yeah. So actually, I think there are some instances in which the legal framework may actually be a little bit clearer than it seems, as far as from a company's perspective, and as far as from Texas's perspective. There are these various patchwork of different types of regulations that these FinTech companies might run into, like the banking regulations and other money transfer regulations.

But at the same time, companies should also keep in mind the fact that deceptive trade practices acts, such as the Texas Deceptive Trade Practices Act, and other states' unfair and deceptive acts and practices laws, do apply to their companies as well. And so they should remember that, even though this is a very fast-paced industry, they need to keep the consumers in mind, and make sure to disclose everything that would be relevant to a consumer.

Especially because, as we were talking about before, that some of the early adopters may not be the most sophisticated of consumers. Though they might be tech savvy, they may not understand the limitations of the services that they're using, such as whether buyer and seller protections are offered, and whether they're going to be protected from third party scams.

So other relevant considerations should be, is this service clearly disclosing the security and privacy options available, or are they possibly misrepresenting the adequacy of their security or privacy? And also, there's a possibility that, depending on the data security of that app, there could be additional identity theft regulations that could become involved as well. But really important to remember that sometimes it is just as simple as making sure that you are not confusing or deceiving consumers in whatever medium that you're using, whether it's a traditional bank, or these new FinTech companies.

DUANE POZZA: Those are good points about consumer disclosure, which we'll go back to a little bit later and talk about consumer understanding of the way that the products work. I also want to, while we're on the subject of the legal framework, get the perspective from the sort of industry side. Do you think that the industry has a good understanding of what the legal obligations are? And would you consider them to be onerous, like an impediment to growth? And in particular, how does the CFPB Prepaid Card Rule fit in? So I'll ask you, Brian, first.

BRIAN PETERS: OK. So a couple of questions to unpack there. I think the broader question of whether it's onus or not, I would say really is more of a question of modernity, and whether the rules are set up for kind of the old paper-based system that we have. If you think about the system of disclosures and liability protections that we have in the Electronic Funds Transfer Act and Reg E, that's all based on your traditional debit card kind of process, where you get a piece of paper in the mail. We'll talk about disclosures in a minute, but that comes in a paper version, and the specifics, even including in the Prepaid Rule, talk about font sizes and what that's supposed to look like.

But we're in a world where this is a screen that is dynamic and that is updatable that can provide a lot of flexible approaches to disclosure, to helping you address something like a disputed charge or transaction. And I think the application to, then, these rules is very challenging, and that it's-- I don't want to use the patchwork quilt excessively-- state to state, when it comes to both licensing and enforcement, we end up with a little bit of a different approach.

And if you think about money transmission, if you're a startup and these startups are doing good things for the space, bringing good things to the marketplace that consumers appreciate and are flocking to, they have a significant challenge going to each state to get a money transmission license. That's a licensing process that they have to go through. Then they have to stay involved in that licensing process every time a feature of their product may change.

And then, of course, there's the enforcement question, which is challenging across all 50 states. So some sort of federal streamlining of that would be significantly helpful. That's just on money transmission licenses. I touched on Reg E on the Prepaid Card Rule, trying to touch every one of your points there. It came out just, like what, a week or two ago. It's 1,600 pages. I haven't read it yet. I will be reading most of it, maybe the CliffsNotes version.

But the thing to think about with the Prepaid Rule is that 98% of the intended effort was what you see in stores, the plastic prepaid cards, that, in many cases, actually come with some sort of a credit component as well. That Rule does capture digital wallets of stored value. We, in many ways, were, I think-- and, again, we're still working through it-- already in compliance with many aspects of it.

So the press kind of made this seem like it was something that was going after digital wallets. But I would say the vast majority of its intent was old plastic prepaid cards. The main aspects of prepaid is adequate disclosure, liability protections, and if you have some sort of a credit component to your offering, that that's also disclosed along the lines of the Card Act.

So you know, we're still working through it to see what it looks like. But there's been a question, I think, that's evolved over gaps for some of these new services and digital wallets. The Prepaid Card Rule, as we better understand it, will probably end up being the thing that we point to say that a digital wallet is certainly under a very explicit regime now that says, these are the rules that you have to follow, and there's not really as much of a question of applicability.

That being said, however, in many ways, our companies have looked at the existing long list of financial regulations, and said it all applies to our services, and we roll out our services and products in a compliant way. We put out a paper in July. It's 60 pages, and it outlines all of those many rules and regulations around payments.

DUANE POZZA: Did anyone else have anything to add?

CHRISTINA TETREAULT: I would just say I'm really glad that Brian made the second-to-last point, which is that the law, the new rules, do appear to apply to stored value in digital wallets, including peer-to-peer applications. Because that was a gap, and that was a concern that we certainly had, when value was stored with some of these providers-- you know, the absence of full protections under laws concerning rate, that contractual protections, while they're certainly better than nothing, are not the same as being able to point to regulation.

And so I think that's going to be a real benefit to consumers when it comes out next year, and could potentially drive some adoption from people who were concerned about whether their funds were truly safe.

MATT VAN BUSKIRK: One quick point, too. Consumer protections are absolutely necessary and any startup that is coming into the space that is seriously trying to do right by their customers will pay attention to all the requirements that are out there. You should have a compliance person as part of your team as early as possible to make sure that you don't get ahead of yourself too much.

But just to reinforce Brian's, one of his first points there, that the rules that every FinTech company is subject to are often-- I mean, they're written for the technology of the time, and then you have regulators-- and I'm also a former regulator-- going in and interpreting rules, applying them to new technology, and trying to figure out how exactly how it applies. And the further in time from the period when the rule was written to the current technology being applied, the more

sort of widely varied opinions you may get by individual examiners who are coming in to try to interpret those rules.

As a FinTech startup, the barrier to entry is quite a bit higher than it is in many other tech industries, which I don't think is necessarily a bad thing, because you don't want everyone to come in and be able to take control of people's financial lives. But it is something to be aware of, in that you can't be a traditional startup coming in, and kind of bootstrapping and developing this. You need to have potentially millions of dollars to spend to go through the state licensing process. Make sure you're meeting all your legal obligations and are adequately protecting customers.

And I think that, if-- I mean, this is obviously a huge challenge to actually pull this off-- but if we move towards having a slightly more agile regulatory framework, like the UK is doing with the sandboxes that they're experimenting with, we may be able to have more of a principles based targeted focus for FinTech companies to be able to meet the consumer protection obligations that they have, but with a slightly reduced burden in terms of the legacy infrastructure.

PATRICK EAGAN-VAN METER: OK. Let's talk about fraud risk. As compared to traditional banking services, do you think that there is a higher risk of fraud on peer-to-peer platforms, and what kinds of fraud specifically? Matt, as the panel compliance officer, would you like to start on this one?

MATT VAN BUSKIRK: I would say fraud-- I was at South by Southwest last year, and there were a number of panels talking about the concept of crime as a service, which is definitely disturbingly a thing. You can go out there, and if you want to create a ransomware virus, there's a tool where you can plug in the specific what do you want it to be called, where do you want the money to be sent, various other customized features-- what do you want the customer to see when you're sending them threatening messages. And then the hacker that created it just takes like a 15% cut off of everything that is received through this virus.

So that's just a micro-example of this, but it's very broad. Every FinTech company that gets into this space is going to be immediately targeted by very sophisticated international criminals, who know, or at least from prior experience can assume, that due to the fact that the company is brand new, regardless of how much they've invested in their control environment, if they're operating with a limited population during their sort of closed beta period, the moment they open the door, they're going to be hit with fraud topologies that they never could have thought of in their wildest dreams, because there are just tens of thousands, if not hundreds of thousands, of these people out there trying to defraud them.

So I would say that a FinTech company is more likely to be disproportionately targeted, but obviously the entire financial services industry is very much subject to this. And a good FinTech that is security conscious can be more difficult, in terms of the protection of their own environment. Since it's a bespoke system built from scratch, they can often be much more difficult to crack than a large bank might be, which has a tech stack that's got systems stacked on top of systems, and thousands of people with access to it.

But you can only build for the fraud you anticipate, and then you need to be prepared with sort of like a rapid action response team to be observing everything that's going on, and have your finger on the switch ready to take a step back and say, OK, we've got a bad pattern. We need to switch to a somewhat more draconian approach for some period of time while we figure out what's going on. And then it's going to be a constant game of chess.

From the other startups that I've interacted with in the past, and from my own experience, you get to be very good at fighting fraud very quickly. But I think we'll get into this a little bit later, too, the weak point, in the end, if you are really good at fraud, is almost always the consumer, and the consumer's devices, and how security conscious they are as well. So you need to be clearly disclosing the steps that you're taking, the steps that they should be taking and such, but we also need to just generally have public awareness continue to increase that you need to protect yourself.

PATRICK EAGAN-VAN METER: And Christina, what are some of the greatest fraud risks that you see?

CHRISTINA TETREAULT: I would say that the mode is new, but the scams are old. And that's really unfortunate, is that it tends to be a lot of the same stuff. So peer-to-peer payments have suffered from the imposter scam. They've suffered from some other types of scams that you see. It used to be sort of Craigslist scams, and now you see them moving into the peer-to-peer applications. And that's where you're selling something. Someone says, oh, I want to buy it, I'll Venmo you the money. Or fill in the blank. It's not unique to that offering. Let me just say all peer-to-peer offerings have experienced this.

And so you provide the concert tickets, let's say, to the buyer. The buyer has ostensibly sent you the money. Tickets are gone, and the transaction is reversed. So you're out your tickets and you're out that payment. And as I mentioned earlier, you can get the notice that the funds are there, and you may even have spent the money, and then that transaction is reversed. And then you're really on the hook, because now you've lost the money, you've lost the tickets, and you might have even incurred an overdraft fee or something else.

I would say, again, from my opinion, and this is based on just monitoring consumer complaints, not only that come to us but in the channels that are out there, which I urge you to look at, the scams look very similar. There isn't something that I've seen that is unusual. And as Matt has mentioned, there's the hacking, and then there's the lack of security on consumer devices that can leave serious holes.

So scary? Certainly. And certainly consumers are well advised to use good digital hygiene, but it's really nothing new under the sun, except the creativity of the scammers.

PATRICK EAGAN-VAN METER: And Beth, as a law enforcer?

BETH CHUN: Sure. So following up with what Christina just said, definitely agree that the scams are often the same kind of scams as in a traditional financial arena. Whereas before, people were maybe wiring money, and now they're Venmo'ing money, or what have you.

And so I think that it's important, again, for consumer education-- I think Matt was already mentioning that before-- that is very important to make sure that consumers understand. Companies need to also make sure that they are disclosing what protections are being offered in their FinTech services.

So for instance, what is this service really intended for? Is it intended to be just sending money between your friends, or are you allowed to use it to purchase something from a merchant? Because those implications do affect what protections consumers have. So for instance, if they aren't supposed to be sending my money to a merchant, then the consumer may not actually have any buyer and seller protections on that transaction. But the consumer may not even be aware of that, because they might be treating the transaction as being more like using a credit card, or something that they are already used to, or are familiar with, having those kind of protections.

And also, as Christina was mentioning, sometimes the transactions might get reversed, or sometimes your account might be frozen. And so really making sure consumers understand when the money actually becomes their money, and what circumstances might impact that, and how quickly are they actually going to receive the money, or is the money going to actually be sent, are important for consumers to understand, too, to help avoid being scammed.

PATRICK EAGAN-VAN METER: And you mentioned commercial transaction. What counts as a commercial transaction?

BETH CHUN: I think that definitely depends on the service that you're using. And so that's another thing that, again, needs to be clear to consumers, what is going to count as a commercial transaction. Is buying something from an individual a commercial transaction, or is buying something from an online store a commercial transaction? I think that may be a more obvious situation. But again, there's a gray area there that consumers need to be made aware of and understand.

PATRICK EAGAN-VAN METER: And what can companies do to combat fraud effectively? And do these efforts encounter a trade-off with the convenience of using the platforms? Yes. Brian.

BRIAN PETERS: I'm the company guy. So we actually take a very different view of this equation. We don't think it is zero sum. Historically, when you thought about payments, it has been a question of signing your signature and there has to be somebody standing there authenticating you. And that is relatively inconvenient.

What we actually see is, because of all of the security features that you now have in an app, online, but especially on smartphones, just a totally different approach to it, so that you can have more convenient payment and more security. And I think just to list off a couple of the things that we're doing. I mean, basically, Matt had a good point about the way this might be a little different for newer companies.

The technology companies I represent have very deep relationships with their customers, and they're extremely good at performing authentication of those users. And then for whether it's a

commercial payment, or a P2P payment saying, green flag. This is a good, valid customer, or user of this payment service. I think we're able to do that through dozens of measures.

But on a mobile device, and through an app, I would just point out that we use multi-factor authentication, tokenization. There is device identification, biometrics, advanced encryption. And mobile security on a device like this is dynamic. You can update it at the touch of a button in a matter of seconds, or minutes. It's not something that you have to mail a new version of in the mail as a new card.

And I think that is just a wholesale revolution in the way we think about authentication and we think about security. We see ourselves, in many ways, as security companies. Financial institutions come to us for security. Government agencies come to our companies, including the CIA, for securer software and services. We feel pretty good about it. It's always an ongoing battle. It's something that I don't think anybody should ever say they're perfect at. But we work very hard on it.

I would say, though, on the startup point that, if you're a new company operating in the technology space, whether it's the financial space or otherwise, you're more likely to be able to take advantage of the latest services. You're going to more than likely operate in the cloud. You're purchasing software as a service. It's very different than what you did 10, 15 years ago, where you would have to invest most of your venture money into an on-premises equipment system, your own data center, and all of your own physical premises security to back that up.

Now, it's totally different. And you can rely on, essentially, the collective technology wisdom of the industry to build your services on a user by user basis, and turn on more security as you need it. There are some differences. But I think it's just a totally different game now.

PATRICK EAGAN-VAN METER: All right, Jo Ann, and then Matt.

JO ANN BAREFOOT: I wanted to reinforce this point, that the advent of so-called big data and machine learning and these very sophisticated artificial intelligence algorithmic learning capabilities is an incredibly powerful solution for both anti-fraud and anti-money laundering. And my understanding from talking with a lot of people is that today the criminals are better than the real customers are at passing the traditional screens. They don't make typos when they enter their identity information, and so on.

And therefore, the newer companies are creating entirely new ways of identifying fraud and money laundering using big data. It's hugely powerful. It's way more effective.

But for the FTC, I think you're the folks who are sort of the keepers of the privacy issue from the public policy standpoint, and thinking through how do you balance the value that we're getting from all this robust new use of data, not only in areas like that-- I don't want to get too far afield from payments-- but in credit underwriting that can be more inclusive is another massive area where more data can be used.

But it does really raise questions about how do we want people's information used, who can get it, what's it for. And it's a hard policy challenge.

MATT VAN BUSKIRK: Just to continue on Brian's point, if you contrast the sort of security components of a credit card, as compared to any transaction that occurs on a smartphone, even with a chip and pin type structure, there's very few elements that a criminal would need to get access to in order to be able to co-opt that whole transaction. If you don't have a chip, then you can swipe the card and then print out a copy of it and go to town for some period time until the person gets a fraud alert on their card.

With a smartphone, the wealth of data that you have is incredible. And then there are startups all over the place that are security focused. I mean, a company like Venmo, Circle, any FinTech company here, can pick and choose whatever they consider to be the best in-class providers, including from companies like Google and such, for OAuth and other systems, to be sure that they really know who their customers are.

I'll give one anecdote of a story I heard here, where there was an investigation where an individual was using a next-gen payments platform to scam people sort of as a fake merchant. They were selling something online, and then not delivering the product, and then just sort of disappearing.

When a law enforcement agency tracked them down, knocked on their door, they said that the phone had been stolen six months ago. But the app has the capability to do device fingerprinting and geo-location, so they could see that the phone was continuing to be used in the same place through the intervening period. So the law enforcement agency could go back to that individual and say, well, you claim your phone was stolen, but it appears to still be in your house. Here's a search warrant.

So there are new capabilities that are unlocked through this that are very, very powerful. And I think we're just at the very beginning of seeing how they can be deployed to improve the consumer protection. But the side effect of that also is the privacy, because the privacy aspect, as Jo Ann mentioned, there is a lot of new data being captured and used here beyond anything that would have traditionally been available using a credit card or other platform like that.

PATRICK EAGAN-VAN METER: Beth, did you have anything?

BETH CHUN: Yeah. Just following up with the security part, and I'm sure we're going to be getting the privacy part in a minute or two. But as Matt was mentioning, the fact that your phone does contain so much data, and it also contains, a lot of times, these FinTech apps in it. And so we should really make sure that consumers are aware of any security options that are truly optional on those apps, and that they should take advantage of those options.

For instance, adding a PIN number or password to that app itself, like you would protect a bank account. And also making sure that the phone itself is secure in case of theft situations. So that way, people aren't just basically getting a blank check book when they steal your phone, so

therefore everything is compromised. So just making sure that those optional security measures are disclosed and used when appropriate.

DUANE POZZA: Do you think that consumers understand the need to take these steps for security? And to what extent are the platforms offering these services educating them about the steps to take for security?

BETH CHUN: I mean, I think that companies are getting better at disclosing these options, but I think that consumers aren't always going to take advantage of them, unless they're mandatory, because they might not always recognize the potential for danger. Like we've talked about before, sometimes these consumers are less sophisticated than traditional finance consumers.

So it's just really important to emphasize to them the importance of your phone is not just your phone anymore. It also has all of these other advantages, but potential risks.

DUANE POZZA: Christina?

CHRISTINA TETREAULT: I just wanted to add, I think there's two things that come up around the conversation for fraud. It's got implications for speed. So a lot of the advantage of peer-to-peer payments and the potential for inclusion that was talked about here really relies on the speed of those funds. And right now, when the absence of real time payments, there are these delays that actually can work to consumers' benefit. Although sometimes consumers complain, and you see a lot of complaints if you look online about holds and delays, those can work to consumers' benefit when it comes to preventing fraud and that sort of thing. And so that's kind of a rub.

And then to Beth's point is there are offerings that have additional security and consumers can take them, but then that gets in the way of convenience, right? And so you have these trade-offs, and it can be tough for consumers, in the absence of experience with these things, to really realize the importance of, say, PIN-protecting each transaction where that's an option, and all.

So I think this is like the thing, to Jo Ann's point earlier, that companies are working on. To Brian's point about a lot of the innovations that are there, it's certainly moving forward, but there is still a lot of work to be done all around.

DUANE POZZA: Brian?

BRIAN PETERS: I'll try to be quick, but I do want to touch on a couple of these points. I think, to Christina's point just a minute ago about some of the delays that are in the banking system, for us-- I mean, this kind of portion of the conversation is really about what matters to consumers and what consumer protections are necessary. I talked earlier about friction. What our consumers find sometimes in using these apps, where there is friction, there is a pain point. It's in the interconnection with the traditional financial institutions.

And so we, I think, want to keep talking about that and look for opportunities to enhance that kind of interconnection. And I think, with respect, delays for the sake of security are, in our hope, something that security can solve. Because if there's a better way to do that and still ensure

that somebody can make a bill payment on time, we ought to figure out how to do that. And all those tools are available now. So if we can just get to a better kind of more consistent real time payment system, with the authentication and the right fraud reduction measures in place, that will be better for everyone.

The, I think, broader point, though, that I'd like to make, and I don't know if we're going to get into disclosure yet, but most of these features that our companies have been working on, I mean, they've taken a lot of effort just from a raw computing power perspective to enable thumb print identification, or other biometric authentication measures. I mean, just let me try something.

Send $5 to Ryan Triplett.

SPEAKER 1: (FROM PHONE) Which app would you like to use?

BRIAN PETERS: Venmo.

SPEAKER 1: (FROM PHONE) What do you want to say in your note?

BRIAN PETERS: Thanks for babysitting.

SPEAKER 1: (FROM PHONE) Here's your payment for $5. Do you want to send it?

BRIAN PETERS: Yes.

SPEAKER 1: (FROM PHONE) Venmo sent your payment.

BRIAN PETERS: So I know that's kind of--

DUANE POZZA: How was that authenticated?

BRIAN PETERS: So that was authenticated with my thumb print. And that all happened through the app that was already authenticated on the device. And there's a whole lot of other layers of security going on there that you just don't have in a traditional payments capability. It's our sense that, as the hardware companies and the software riding on that hardware works to make all of those features available, it's a difficult question to decide whether that kind of functionality and that kind of security should be on by default. We want to meet our customers where they are with what they want.

You think about all of the discussions that a company like Apple has been through when it comes to security recently. Payments, health, our most intimate personal photos, those are all the reasons that we're building security into these devices. And it's frankly one of the main reasons that peer-to-peer payments are taking off. I think customers now see this as a secure kind of technology that will allow them to do that.

And the screenless transaction that I just did-- I was looking at it-- but there is a world coming where you can do that through all manner of IoT devices. And the authentication, and also, too,

the disclosure, is going to be a very interesting topic as we look to that level of both security and payments without screens.

DUANE POZZA: We're down to our last 15 minutes, and I want to drill down to at least two more things, and then sort of have an open-ended other things to talk about at the end. The first one is privacy, which we've touched on a bit. We talked earlier about how some of these platforms have social media components, but more generally there's a lot of financial information that's being collected. And my question is, how well do the platforms do at disclosing the ways in which this personal financial data might be shared? And are disclosures sufficient for consumers to understand who might get their hands on the data about their financial history?

BETH CHUN: So I think that it was very interesting having that Venmo demonstration there. It did actually highlight some of the privacy concerns, which is he said send money to this person to pay for babysitting. Now, depending on how the app settings are, the fact that he sent money to that person and what he sent the money for might be broadcast to the whole public. There are different options on some of these payment transfer services that actually allows you to make it into a social media component to it.

And so it's really important that people remember that, and that they fully understand the privacy options that are available to them on these services. From before they even download the app, if it is an app, then they need to be checking out what permissions that they are giving that app to access on their phone. They should read any relevant privacy policies.

And the apps themselves need to make sure that they are doing a good job disclosing different features that they might have, especially if they differ from what a consumer might expect. If you don't expect that your money transfer service is going to act as a social network, then that needs to be very clearly disclosed. What are they going to do with your contact information, if that's one of the permissions that you're providing. And that disclosure probably should be made in multiple places to make sure that it is really clear to consumers how their privacy is being affected in new and different ways than they might be expecting.

DUANE POZZA: Anyone else on that?

CHRISTINA TETREAULT: I would just say that strong disclosures are certainly important. There is the difficulty on a small screen of trying to convey super important information. So that's one piece that I think is certainly a wrinkle here. And then some of the defaults are not privacy protective, and so the concern is that consumers may unwittingly end up exposing more of their information than they care to. So I always urge consumers to choose the most privacy protective settings possible, particularly given that, although you may think you know your friends, you may not know them that well. And given the sum of liabilities.

Yeah, the privacy piece, I think, is critical also for reasons that we've already talked about. It can make you a target of fraud attempts, and that sort of thing. Your information, like even your email address, or your phone number, now becomes a phishing tool in ways specific to these services. And so it certainly expands the target that you have on your back already for scammers.

BRIAN PETERS: If I can respond real quickly? I think, if you look at, at least with two of the apps that I work with, Venmo and Google Wallet, the features and the disclosures that Christina and Beth are talking about are just either two or three taps away. If you have a concern over a transaction, three taps and the phone is ringing to somebody at Venmo. If you want to find out more about how to adjust those settings, it's right there, and it comes up-- yes, it's a small screen-- but in a clear, kind of concise, way that is understandable. What I think the private sector companies are always kind of trying to do is find a balance between what makes sense for as many users that they have as possible, and also what regulators have as interests in essentially ensuring some sort of kind of baseline setting.

Now, the hard part, when you start talking about that from a policy perspective, is that baseline may not be adequate, and it gets outdated very quickly. So we think about disclosures again, and we talked about the Prepaid Rule and everything. You know, the concept there is that you get a big piece of paper in the mail every month, or once a year. You can do so much more, in terms of better disclosure, much more effective nuance, just in time kinds of disclosure, offering consent opportunities at every given moment if that's what the consumer wants, all because that's possible on this device that it never was capable before.

And I, unfortunately, would like to see more recognition of those possibilities in some of the rules and regulations that are being contemplated. I do want to say that, for the CFPB Prepaid Rule, there is some contemplation of that. Cordray, in a speech just a few days ago, pointed out that, with respect to disclosure specifically, they want to be creative and they're open to that, despite the fact that they're trying to be consistent across a lot of history and historical precedent.

PATRICK EAGAN-VAN METER: And following up on that, Christina, do consumers know who to contact when something goes wrong? What are the methods of contacting the platform?

CHRISTINA TETREAULT: So this sort of stretches across all the issues that we've talked about. It really depends a great deal, as I said earlier. The offerings vary tremendously in terms of the amount of help that you're going to get or who you can contact.

I was using one of the apps that I have and I wanted to make sure that I had the most up to date disclosures because they do change quite a bit. And I couldn't find them. And this is a place that I've been before and a thing that I use. Then, I emailed, because there's no phone number. I did the in-app communication, and I still didn't have a response 12 hours later. So I don't know that I have the most up to date information about that particular service. But I find it noteworthy that there was no way to talk to another human being about what the issue was.

So it can really vary whether consumers have access to the information they need. So that's sort of the baseline, and then to your more specific question about whether consumers use it. I think that's the wild card. A good disclosure will never save a bad product. In these instances, because of the variety of cross offerings, that also is very difficult. So although I've made some sort of blanket statements about what consumers should do, they may or may not be able to do those things, and they may or may not be able to easily or quickly find out what that particular channel is using when it comes to, say, privacy settings or protection, security, extra security steps that they can take.

There's one other piece that merits mention here, is a lot of these agreements have arbitration clauses. And anyone who's followed some of the recent banking scandals knows that those very particular consumer concerns. And that's another aspect of-- even if you uncover a problem, you may or may not be able to have a remedy in court.

And then the question around whether consumers take these steps also raises a question about what liabilities the consumer incurs. And some of the services very explicitly limit their liability to consumers for $1, or the cost of the transaction in some instances. And there's others out there. But they also have provisions for fining consumers for misuse, which I thought was super interesting, because you don't see that a lot.

And so, again, whether consumers know these things, I don't know. And I think that merits further study. It's not just a matter of are the disclosures clear, because, of course, that's certainly important, but I think consumer testing to make sure that there is comprehension is really critical. And I think, to Brian's point, there's a whole new mode and a whole new way to look at this, and it certainly merits a lot of experimentation, investigation and trials, and hopefully some solid research that points the way forward.

PATRICK EAGAN-VAN METER: And Jo Ann, responding to that and kind of following up on some of the different threads, do you think that the ability to get a quick response would help broaden the adoption of some of these payment solutions?

JO ANN BAREFOOT: A quick response on your questions about privacy and so on?

PATRICK EAGAN-VAN METER: Or any sort of query to the platform?

JO ANN BAREFOOT: Yes, but I think the problem is more fundamental than this. I'm spending two years at Harvard writing a book about financial innovation and regulation. How to regulate it, how not to regulate it. I've been a regulator. I've worked for the US Senate. I've been a consultant in this space forever. I don't want to hurt anybody's feelings, but I have reached the conclusion that the disclosure model, which I myself have contributed to over the years, is not very effective. I'm not saying it's useless, but it's not getting us where we need to get in having consumers-- nor is for traditional consumer financial education.

And today we have technology that can really rethink how and when we give consumers the information they need. And it's not going to be a product -- I mean, even if you look at the product disclosures on privacy, how do you know what your answers mean to you? You want to use the service. Is it going to cut you off from something you're trying to do? It's befuddling. It's very, very complex.

But these are phone-based services. Peer-to-peer payments is embedded in all of these powerful options that are coming into the phone. And with them is coming to have your phone take the initiative to coach you, to warn you.

I saw a demo the other day of a new consumer financial management app-- it's actually a broader suite of services than that-- and the scenario is you say to your phone, send Richard $50 on

Venmo for dinner. And the phone says, OK. Then she-- I don't know why it's always a female-- she says, do you have time to talk? And you say, yes. And she says, if we send Richard $50, you won't have enough money to pay the rent at the end of the month. Can Richard wait? And you say, no, pay Richard now. And she says, OK, I'm paying Richard. We're going to take your daily spend from $50 to $40, and I'll keep you posted on how it's going.

The technology is there to take the initiative, to not wait for us to go say should I look at my privacy settings and what do they mean and who should I call, but to actually warn you and coach you at the moment you have to make a decision. And how do we create the incentives for the industry to build those kinds of tools, that the phone says to you, I see we're at the grocery store. We've got $75 to spend here today. Or I see you're walking toward Starbucks and you already spent your whole Starbucks budget, so keep walking.

You know, this is there, and the question is, how do you get it in there aligned with the incentive to help the consumer, instead of get them to do things they shouldn't do, which is what some of the financial models of the past have been about?

DUANE POZZA: Last question, as we're reaching the end. Is this an industry where you're likely to see some sort of self-regulatory regime, voluntary best practices, or even sort of an attempt at meeting of the minds among the industry players to address some of the issues we've talking about? Is that a good idea? Is it a bad idea? Too early to tell? What do you think? I'll ask Brian first.

BRIAN PETERS: I think it's going to be a little bit of everything. I mean, clearly regulators, consumer advocates, companies, and the like are all a part of this discussion. There are best practices efforts out there. I think an interesting one that I just saw last week was the Consultative Group to Assist the Poor put out a report recommending UI interfaces-- user interfaces-- for their community, which is basically trying to make sure that all of these new apps in developing countries-- because these are developing on a country by country basis, because financial systems are generally closed on a national basis-- are trying to kind of figure out what works best across all of these countries. And so this is, I think, a great effort. That's just one example. The FIDO Alliance is an interesting one working on authentication, trying to get past the password, looking at multi-factor authentication. That's just a couple.

I think those are good efforts. There will continue to be conversations between our companies and regulators, both on the policy front, but as well as how to enforce effectively.

DUANE POZZA: Beth?

BETH CHUN: So first, I wanted to respond to something that Jo Ann said, and then I also have some comments related to what Brian was saying.

So as far as disclosures go, I think that, while they are definitely part of the solution, they may not be the only solution. But also making sure that disclosures are keeping up with the technology as well. Kind of like what Jo Ann was saying, if you can have the disclosures be at the same time-- and this also relates to what Brian was saying-- if you have the phone here, if

you can make that disclosure at the time you're making the payment, then that's very helpful. And if you can just make sure that the disclosures are being made in ways that are relevant to today's consumers.

So maybe the example before of the disclosure being made in the mail is not particularly relevant to a mobile app. But you can update that to actually be on the app, be also through email or other ways that consumers today might be more likely to access those disclosures.

But as far as industry best practices, I think that those best practices, should they be developed, could be very helpful for regulators as well. We do use best practices as a tool to help us identify which companies are outliers. And if they're not following the best practices that have been set out by the industry, then often that's a clue to us that maybe this company is not following the law either. They may be violating unfair deceptive acts and practices laws.

So another potential avenue, as far as the fact that there maybe aren't industry best practices right now available, especially for really new, really innovative technologies, it can be helpful to approach some of the regulators to get their opinion on that service. Of course, they can't provide legal advice, but at least the regulators can, then, ask questions about that service, and it might give a new perspective to that company regarding what things they might want to think about in working to start this new business, and what potential consumer concerns that there might be.

DUANE POZZA: And I'd echo Beth's point as well. We always like to hear from all stakeholders across the industries as these things develop. It's very helpful from our perspective, and for everyone's perspective.

So thank you. We're out of time. Thank you so much for our panelists. It was a great discussion.

[APPLAUSE]

Coming up next is a presentation on crowdfunding by Christina Yeung of the FTC Office of Technology Research and Investigation.

CHRISTINA YEUNG: So good afternoon. Today's presentation will go over our survey of 20 crowdfunding platforms and their online practices.

So what is crowdfunding? Simply put, it's a website or online portal where anyone can either create a campaign to collect money or find a campaign to give money to. The goal of our research was to find out what, where, when, and how consumers find information as they navigate crowdfunding platforms.

The outline of our presentation today-- we'll start with the scope of our study and go into a little of our methodology. Then, a quick industry review, where we'll go over general observations about the 20 crowdfunding platforms. Next, a look at the consumer experience and the information available to a typical consumer. Finally, potential dispute resolutions, such as refund policies, how to contact the campaign organizer, and a few other points.

So how do we choose the platforms? We started by gathering our initial list of crowdfunding platforms by looking at five different aggregator sites. These aggregator sites compile curated lists of crowdfunding platforms. From these, we narrowed our study to those that appeared commonly across the aggregators, excluded companies with no US presence, and choose the top 20 based on their alexa.com home page ranks. Alexa is a service that provides commercial web traffic data for most sites.

We visited each of the 20 platforms, and should note that, of the 20 platforms, three of them were active but had no current campaigns. This means that, even though we are able to browse through the campaigns, the deadlines had already passed. With our finalized set of 20 crowdfunding platforms, we began to look at general business models.

We first started by collecting information from the home page and moved through any subpages or archived links accessible from the home page. We also used Google to search for relevant information, but limited the results to the domain of the crowdfunding platform. Privacy policies and terms of service were not included in our study.

So what did we find? Crowdfunding platforms in our survey fell within two parent models. 10 fell into the charitable model, in which consumers give money to campaign organizers without expecting anything in return. Three fell into the second category, rewards, where consumers give money with a promise of goods or services in return. Seven of the 20 platforms present rewards, but also gave consumers the option to simply give money without requesting anything in return. These fall between charitable and rewards based models and are represented by the overlap you see in the graph above.

Next, we looked at how campaign organizers could collect money on these crowdfunding platforms. Again, platforms in our study fell into two primary models. First, the keep it all, where campaign organizers could keep all the money donated through the platform with no built-in requirements. Some categories of keep it all include pledge, where consumers make a one-time donation to the campaign organizer, or subscription, where the payment can be spread across months. The subcategories get more complicated, but for today we'll stay at a high level.

The second model, the all or nothing, forces campaign organizers to meet their funding goal within a specific deadline. Otherwise, they don't get to keep any of their funds. Three platforms offered both types of collection models, but made campaign organizers commit to one model or the other prior to launching their campaigns. This means that campaign organizers on those platforms cannot start one of their campaigns with all or nothing, realize they weren't going to meet their goals, and then switch over to the keep it all in an attempt to keep all their funds.

So now we've covered payment and collection models. Let's see how they're used together. In this graph, what you're seeing across the bottom is the different types of crowdfunding platforms. The charitable, the rewards, and the rewards with donations. The vertical axis shows the count of our platforms of our total 20 observed. Keep it all is represented in blue, all or nothing in red, and platforms that offer both options are shown in green. As you can see, the majority of our charitable platforms in our study offered the keep it all model, while the rewards platforms, and the rewards with donation option, lean more towards the all or nothing.

While studying these platforms, we noticed that most of these commonly disclosed two types of fees somewhere on the home page or on linked pages. And the fees that they disclosed include the platform fee, which breaks down into a fixed flat percentage, and a payment processing fee, which breaks down into two components-- a flat fixed percentage on a per transaction fee. We observed the platform fee discussed on 19 of our 20 platforms, and saw the payment processing fees disclosed in all of our platforms.

We also looked at whether or not platforms limited how long campaign organizers could collect funds. On this graph, again, along the bottom, you see the different types of platforms, the charitable, the rewards, and the rewards with donations. And the vertical is still the count of platforms.

Campaign length limited whether there was an expiration date after which campaign organizers could no longer collect funds is shown in blue. If a platform allowed campaigns to collect funds indefinitely, it's shown in red. As you can see, platforms in our study tended to have no limitations on how long campaign organizers could collect funds. Green represents platforms that allow campaign organizers who met their funding goal within the initial deadline to continue raising funds afterwards. Rewards and rewards with the donation option offered this possibility.

The second half of our study. We take the role of a hypothetical consumer and try to get an understanding of what information is available to them through the campaign pages of these platforms. For each of the 20 platforms, we selected five campaign pages. So in total, we looked at 100 campaign pages. These campaigns were all either directly promoted or indirectly linked on the home pages of their respective platforms.

So what did we find? Depending on the platform, campaign pages will have dedicated fields for different pieces of information. For example, on all of the 100 campaign pages, we found these four pieces of information. We observed a project title, the campaign organizer's name, an image or video associated with the campaign, and the description box. The description box often appears as a free form text box, where campaign organizers can include as much or as little information as they desire.

There's additional information that we observed on campaign pages that did not always appear on every platform. So what you're looking at in this graph is, across the bottom of it, are pieces of information that we found fairly commonly, appearing on 10 or more platforms. And the vertical axis is the count of the platforms out of our total 20 studied.

In this graph, if a piece of information was observed across all five campaign pages in a platform, it's shaded in blue. If we observed it on only some of the campaign pages, it's represented in red. For example, on 19 of our 20 platforms, current funding was disclosed on each of the five campaign pages of every platform. On the last platform, we have sometimes observed the current funding on some of the campaign pages, but not all. So it's shown in red. The green category represents if platforms allowed campaign organizers to restrict information to people who had already given money to the campaign.

You can see this in the update section, where one platform allowed campaign organizers to limit who can see the updates to active supporters of the project. So people who hadn't yet given money were not able to see those updates. In comparison, the comment section of the campaign page was always visible to consumers. However, some platforms also limited making new comments to active supporters of the project as well.

A small note. For our purposes, we looked only for the information provided in dedicated fields. A campaigner can always include as much or as little information as they want in the free form description box, but this is at their own discretion. We only cleared a platform if it provides a dedicated field for disclosing a given piece of information.

So the layout of this graph is the same as the previous slide. However, along the bottom of this graph what you're seeing are pieces of information that we observed on 10 or fewer platforms, while the vertical axis is the count of platforms. Certain pieces of information, such as the organizer's bios and the history of the organizer and the platform, as seen by the number a list of projects created and backed, are still fairly common. However, as you move further right in the graph, items such as automatic identity verification disclosures become much less common to find.

In addition, some platforms provided a field they called social media verification. But whether it meant that the campaign organizer had gone through an additional step of identity verification, or whether it simply meant that they have just connected a social media page to the campaign was not always explicitly disclosed.

There were some fields that we observed that were unique to platforms using rewards based payment models. So on the bottom of the graph, you're seeing those fields. They include an estimated delivery of rewards, whether or not platforms give campaign organizers the option to limit the number of rewards to a specific number of consumers, the current number of backers within each reward level, and shipping limitations of each reward.

One of the things about charitable platforms is understanding who the final recipient of the funds is, and sometimes it differs from the campaign organizer. A field unique to charitable platforms we observed was one dedicated to the beneficiary name, where campaign organizers could list who would ultimately receive the funds. On three charitable platforms, this was always observed across all the campaign pages. On four platforms, it was sometimes observed. On our remaining three, we never observed this field.

Looking through the campaign pages, we noted significant difference in the language platforms used to describe making payments. By the language, what we were looking for was the actual button that consumers can click to continue the payment process. As you can see in our study, charitable platforms were more likely to use the word donate, while rewards and rewards with donation platforms, as seen by them booth on this slide, use a greater variety of words, such as pledge and fund.

So after researching the campaign, what if our hypothetical consumer wants to give money to the campaign? To answer this, we attempted payment through each campaign page when the option

was available. We found that 17 of 20 allowed payment through debit and credit card, of which most used WePay and Stripe to process the transactions. And of the 17, three also allowed payment through check. Six additionally provided an extra option to pay through PayPal as well. Three of our 20 platforms used only PayPal to process transactions.

So as you recall, we were looking for information in other parts of the website, such as the home page, about fees. We found that most crowdfunding platforms disclose a general fee structure consisting of the platform fee and the payment processing fee. In comparison, we wanted to see what fees are actually disclosed during the checkout process, once our hypothetical consumer actually decides to make a payment to the campaign organizer.

We reviewed 18 platforms, as two of the platforms were live. But we observed no campaigns we could actually donate money to, so we couldn't complete the checkout process on them. Of the 18, we observed some sort of fee disclosed on seven, while on 11, we did not observe any fees disclosed at all.

Of the seven that did disclose fees, they broke down into five charitable platforms and two rewards based platforms. Of the charitable platforms, we observed that three disclosed the platform fees, while two disclosed a combination fee of platform and payment processing fees. We observed shipping fees disclosed in the two rewards platforms.

We also observed, of the seven platforms that disclosed fees, six of them added fees to the total donation by default. For example, if our hypothetical consumer decided to make a payment of $100, and our hypothetical fees totaled 15%, six of the platforms would add $15, making the total payment $115, while the last platform would subtract $15 and give the campaign organizer $85.

Finally, four quick points that we pulled aside about potential dispute resolution. We observed that these points were not reliably found in any one place and could be listed in very different areas across the crowdfunding platforms. The first of these points is where to report a campaign. First, we looked on the campaign page. Five of these platforms had a dedicated button for reporting campaigns. Next, we looked on the frequently asked questions and help sections. Three additional platforms provided instruction on how to report campaigns to the platform. We did not observe any way to report campaigns on the remaining 12 platforms.

The second point is one on how to you receive a refund. What if our hypothetical consumer changes their mind and wishes to withdraw their payment, but the payment has already been processed? So in this graph, along the bottom, you're seeing the different mechanisms we observed platforms used for refund policies, and the vertical axis is the count of platforms.

We found that 10 of these platforms instructed consumers to contact the campaign organizer directly, and that refunds are made at the discretion of the campaign organizer. Three of the platforms provided guidance on how to contact the platform, but made no guarantees. An additional three simply said there were no refunds available on the platform whatsoever. The next three, we observed no refund policy. And in the last, we observed that the platform instructed consumers to contact the payment processor to facilitate any refund requests.

One last point, canceling payments. What if the payment hasn't yet been processed? We observed four allowing canceling under specific conditions, such as if the deadline had not yet been reached, or refunds had not yet dispersed the campaign organizer. As a side note, some platforms actively monitor campaigns and make sure that they meet specific standards. What the methodology is behind the monitoring process is not always explicitly stated and seems to vary across platforms.

So what can consumers do? Check out the FTC consumer guidance, such as the link below. These slides will be posted on the website at a later date. Listen to today's panelists for good conversation. And thank you very much for listening today to the presentation.

[APPLAUSE]

EVAN ZULLOW: All right, thank you very much, Tina. And as you can all see from the prominent slide behind me, we're going to be taking a short break until about 3 o'clock when we will convene the second of our panels. Thank you.