James Van Dyke

Male Speaker:
This is about verifying identity, and it's one of many security-related mobile finance apps. We will give individuals much more control of their security and not just be protecting them from bad things but helping them protect themselves and be empowered as consumers and businesses in ways we haven't seen before. Certainly mobile banking, which is absolutely here to stay. Data makes it very clear. If you're wondering if mobile banking is the real deal because just like with the first time that we had online banking, that was experimented with back in the 1980s, it failed and we retrenched and then came out with it in the mid '90s and then it succeeded, mobile banking, we're on version 2.0. All those companies, literally 100 percent of the original set of vendors, came and went.

Now, that we're back, if you look at iPhone users, half -- one out of every two -- iPhone users are now doing mobile banking on a regular basis. I don't know about you, but that number shocks me. And yet that iPhone population group, if you want to follow an indicator of future usage patterns, you really can't look to classic indicators like age or income. Mobile finance usage defies those categories but iPhone users, who span a lot of diverse categories, will tell you what everybody else is going to be using next. So we define that as monitoring and managing finance at the simplest level.

There's mobile commerce in shopping, which is buying via the mobile device generally for the mobile device. Very different than this last item which we call mobile wallet. We call it a lot of different things but if I'm downloading your ringtone or a screen saver or something like that that makes my mobile device itself work better, I mean, that's so common and it's been around so long, this is a part of mainstream today. There's mobile marketing which gets really interesting and is another app that along with authentication that uses geo-location. So, you know, we're really hindered by a very rudimentary U.S. telco system compared to other modern economies around the [inaudible]. But as we get more geo-location capabilities and fatter pipes underneath the system, underneath the devices, then we'll enable more attraction, cross-talent, keeping customers by mobile devices and something we called for a long time just happened a couple weeks ago, Wells Fargo actually treating the mobile channel, finally, as an entirely distinct channel where you can sign up and get a mobile banking account separate from an online account. We're the only bank that offers that in the U.S., and prior to that, nobody offered that.

There's mobile payments which, again, define this any way you like. We're defining it as one person sending funds to another person. It's been around a long time. It's been available a long time. Talking to Dixon [spelled phonetically], it was PayPal's original model when they were started and they said, really, the other model has worked out a lot better for them, you know, which is auction-based payments via desktops and laptops. But, of course, they've been offering that a long time.

But now we're starting to see growth. This is an example where your older demographic models are saying let's look to affluent young people, especially males, they'll be the early adopters. Just defies all those traditional rules because you see underserved and

underbanked consumers showing some of the highest levels of interest, and this is where financial services can really get back to being about services. You can replace some other businesses there, offer some more questionable value propositions like check cashing services and so forth.

There's a mobile wallet area where we really could leave the wallet or the purse at home and not really be sorry we did, maybe not really notice that we did for a couple of days. Let's face it, the photos, the notes, all that stuff are on a mobile device for a lot of people. I don't know about you, but for me, they're already there. And as we get to that and as we load in all these other things that lay the rails, then we'll get to the mobile wallet.

So, I'm not going to get to details on this slide. There's just a lot here. It's really a leave-behind for you but I just wanted to let you know we divided this up and as Marianne and I talked about dividing up the content, going to break up the different models on the left, the right and the top. SMS [spelled phonetically] text which is really like a separate way of interacting with your financial or payments provider. Then using WEP [spelled phonetically] and browser-based banking and some phones allow that more than others, some networks, some plans. Security is an entirely different animal than downloadable applications which the world has been changed by that by iPhones and Droids and Trees [spelled phonetically] and, of course, Blackberries. And then embedded applications which allow telcos which everyone's wondering are they going to be the next financial community that needs to have a different set of regulations and oversight attached to them? So these all work very differently, and there's different consumer and business models, and you've identified some of that.

So if you look at the ecosystem at the broadest level, there's a mobile subscriber. We generally think of consumers when we think of this, but we could just as well be thinking of business users. And we talk about wanting to protect this person and say sometimes the best way to protect this person is to do what we call deputizing this person because a lot of the best banking systems, the most effective banking systems at stopping this identity fraud crime, sometimes called identity theft, it just doesn't go away. This year a report we just came out with a couple of months ago acknowledged the FTC's original good work in the design of that and sheer wells [spelled phonetically] and intersections and fi-serves [spelled phonetically] and the Better Business Bureau being part of that release. When we did this project we found the latest ID fraud numbers in the U.S. just on the amount of the crime was 54 billion dollars. Good news is the consumer is only paying $373 out of pocket. I mean, it's bigger than zero so it's bad news, but it's a lot lower than people think because the business community is paying, on the average, $4,851 per spree of inter-related crimes. Business are paying all but $373 so this is a big cost that no one is talking about and that doesn't count the cost of all the mitigation systems that protect, prevent and resolve the crime.

But we believe very firmly that it's not a whim. It's what we see in the data or we look at the patterns of the crimes that the best way to protect this consumer, or end user, the financial account holder, the identity holder, is to actually empower them and see that technology is a two-edged sword because some of the best -- completing a thought I was

on to a moment ago -- some of the best back end technologies and methods, fraud filters, neural nets, all this stuff, fundamentally what they're doing is trying to think like the customer. They're trying to be like this big brain that would say if you had the customer right there, instead of using a technology, you'd say, oh, is that you? Are you out of the country right now? Do you want to approve that transaction? We're programming systems to think like the customer. If the customer's right there we'd say is that you? They'd go, no, it's not me before the computer could respond and much more accurately.

So as mobile devices are connected to individuals and they're actually standing in the line buying the item, why wouldn't we just send somebody a message with the strongest authentication and give people alert messages which we're going to think I'm a little bit out there when I say this, but rather than working like they were financial alert messages which by one criticism about current banking systems is that the alerts are really very bad today. They're incredibly ineffective and we have a press release out on that today but they don't require much changes to make them really phenomenal. The way they need to work is actually a lot like how people manage their music electronically. You get a message, you get a song, you say I want more like the one I just heard. Well, that's like that next one and you're constantly --

[laughter]

-- aware of how much money you have as a consumer or business account holder. You have this ever-present awareness and if you're in Brazil and you don't want your card shut off, you're financial provider does it and if you're not in Brazil and you don't want a slew of transactions that after $4,800 all of a sudden be committed, those don't happen. So that's how we empower the customer. That's what we've seen in our data.

So mobile operators, different versions of a phone plan of a sort. Let me -- can't see this over here but -- but SMS, WEP, downloadables, all that. You know, and the one thing that, some of the reasons that we all as people that have worked hard and our education, professional experience and all that, so often get some of this technology wrong is that, you know, when you think about simple numbers, you see some major change happen that you've been working on and, I don't know about you, but I generally get about, from the gut feeling, I get about half of it right, you know? There's a lot of things that we as an industry have sometimes been right on, sometimes not. Consumers or business owners, they don't want to be -- they don't want to have their convenience disrupted to be more secure. That's true. And yet we all often hear things like -- I'm just making the point about not getting caught up in pre-conceived notions that actually cause us to make bad decisions, whether that's commercial decisions or regulatory decisions, what have you.

Has anybody ever heard the urban legend that zero liability policies cause consumer motivations to go down in terms of protecting themselves? Would you be surprised to know that actually the opposite is solidly true? Those individuals that most value zero liability policies, which come from $50 liability limit regulated policy, those individuals that most value that actually are most vigilant in taking other measures to protect

themselves. So it would be true to say that zero liability policies actually cause more individuals to be more active in their own self-protection. It would take a psychologist or behaviorist to explain why that's the case. That's not what I do, but the point is a lot of those pre-conceived notions can get in our way.

So when we look at how all these providers play out, if we were to take 50 percent of our accuracy rate on the next technology, multiply that four times over and as industry rolls out, we'd be six percent correct after four major waves of technology. And our point is that mobile will change things a lot and we have to make sure we're grounded, in fact, to have good policy decisions.

When we look at this end game, if you will, because -- I'd love to hear anybody's comments later on if you have a thought -- but, you know, when I think about a mobile finance rolling out, it's hard for me to imagine a bigger end game than people leaving the wallet or the purse at home. And in everything else, every other mobile finance app we identify really rolls up to this, and we think this can be great for business, great for consumers, great for just us as a strength for the country, but there's so many things that have to change in order to have that happen and so much experimental new technologies. And one of the key things, because this involves a lot of alternative payments, as they're often called, you have to decide what's an alternative payment? So, for example, is PayPal an alternative payment? Well, in its realm, it represents about 90 percent of the payments that are done in the area in which it's strongest which is auction-based payments and all those other auction users that send funds from one to another.

So you can argue about what's alternative and what's mainstream, but I would say this. If we want to identify through a model which alternative payments providers are likely to succeed next year, year after that, what we found to be a tried and true model for having a highest accuracy rate is to look for a balance value proposition. Look for an alternative payments company that offers the most balanced, not necessarily the strongest, value to any one entity or entities meaning consumer or small, medium business user, the merchant community and the financial issuers that roll this stuff out, those three primary communities. If you look at all those three and you say what's the value proposition of one alternative payments provider in this model, we'll see just a flood of them coming out -- which is why I'm talking about them -- that's the best way we've found to be predictive, you know, in terms of who will succeed and business models will succeed.

And certainly security is going to be just crucial as we go through all this as well. You know, there's a lot of surprises about security, particularly in regard to data breaches right now. We have been among the voices saying for a long time that we couldn't find a correlation between data breaches and actual consumer likelihood of becoming a fraud victim. And so you hear that coming out a lot. Others started saying that as well and then we had to actually do a 180-degree change in our position because actually as we looked at data, actually brought a new statistician on and looked at actually some old data, I'm kind of embarrassed to say, I was looking back over a couple of years of data, just dusted some of it off and we said, you know, we missed something. Looking at, you know, some longitudinal data history, and found that actually there was a four-times

increased likelihood of you becoming an actual fraud victim, real fraud, not just a victim of a breach, but actual fraudulent transactions if you get one of those data-breach notification letters. I point that out because that's our trigger for knowing the individual had a higher likelihood of becoming a fraud victim. Of course, there's regulatory policies that determine whether you get a letter or not.

So the point is, as we looked at the data more extensively, we found this and we have a real problem on our hands with data breaches which relate back to a lot of the end points like merchant communities and acquiring community where some of the largest data breaches have occurred and other areas like that. So they're actually not occurring as frequently [unintelligible] at banks themselves but that's where a lot of the brunt is being felt and then you can argue about whether the loss is being incurred.

So this is a complex slide. I'll zero in on just a couple of simple areas which is this point as well and start to hit on it sort of repeatedly. I just find from a regulatory standpoint, particularly, this point about empowering the end-user. It's not just a nice-to-have message. It's really a need to have for just the protection and the good of everyone. So here's where it gets interesting. Yes, it's nice to say those broad-brush things but what do you do about it?

Well, we look at the security impact of various apps, and I'm using slightly different language, thanks to your patience here, for the purpose of pointing out where the security opportunities or threats, kind of a mini-SWOT analysis, if you will, strengths, weakness, opportunities, threats from apps on the left side, so mobile marketing, alerts, authentication -- fourth down -- review and release alerts where the account holder or maybe the identity holder where you're trying to protect against new account fraud and alerts aren't just about security. That's for sure. They're also about helping people work toward financial goals, to just have more convenient access to their funds. So once we get alerts to send a message out to someone that they as an individual can respond to, which can go horribly wrong if the security isn't in place because maybe we're allowing the criminal who has their hands on the phone to do the responding and say, "Yeah, that transaction is okay, and by the way, lift all my previously instilled limits on those foreign transfers. Just open them all up. Thank you." So, yeah, these can be a horrible thing or they can be a wonderful thing by taking all these smarts, these big-brain neural nets, fraud filters, all that great back-end stuff, device fingerprinting and then getting the individual to be plugged in on that.

But the review and release alerts -- here's my point on this -- is that if we accept the idea that empowering the identity holder and the account holder, consumer, business, whatever is a great way forward for effectiveness and new business models and safety that I think will really finally drop this ID fraud number that has never gone down since, you know, the FTC first reported on it in '03 and we've been reporting on it for six years since. It doesn't really dip below 50 billion and that's easily a hundred billion crime out to the financial community when you look at the litigation costs.

So this review and release part, I think is the key that gets us out to mobile payments because once you have people having access to their financial accounts and they can respond to real-time messages -- somebody's thinking well the real-time systems aren't there -- I know. But this is where real-time systems have a value proposition that they've never had before, the core banking system, real-time system. I worked for real-time banking systems, for credit unions, I don't know, 10 years ago or something like that -- twelve years ago -- and it's a big so-what in the industry. But once you connect it out to the end-user it becomes relevant along with so many other things. Aggregation technologies start to get relevant. So payment transfers, all this stuff. So the point is that the security has many plus-pluses or minus-minuses depending on which application we're looking at.

And the adoption is very different and everything from review and release alerts which I've seen television commercials for some banks today and I could swear they'd be available and yet I can tell you from day-to-day action they don't exist. But they're in a few parts of the world, like South Africa and a few places in Eastern Europe where fraud is just out of control. By and large, they mostly don't exist at any kind of practical level and there's others that are growing very fast like mobile banking by 50 percent of the end-users.

You can also -- I will tell you that there is opportunity to mine some of the data and make great policy decisions whether you're a financial services vendor, policy maker, payment provider, whatever. And a great example -- I don't know if it came from a meeting I had, and I'm hopefully not trading on any confidence or anything -- but one of the last times I had the privilege of presenting before Board of Governors was probably about five years ago, and I had said some similar comments about saying -- let's not just go too far with just trying to be, the word is paternalistic or protecting the consumer, but also think of empowering the consumer because they want to get involved and the tools just aren't being shared with them. And somebody had said to me, kind of in a question and answer in front of a group similar to this size, well, what could we do or are there any opportunities for policy that don't exist yet that you see from your data where one policy decision could really make a difference?

And I had a big, thick ID fraud report and said yeah, we see an unbelievable correlation between address changes and ID fraud. So if an address has been fraudulently changed you are much more likely to have the worst form of ID fraud occur and the most damaging in terms of hours and out-of-pocket losses to the financial community, consumers and all that. And address changes red-flag rules were talked about at that time, and I don't remember of that conversation a long time ago actually had to do with this change being made. Now, we see a very positive thing and I mean where great public-private cooperation happen and when we look at that, we actually have banks that have notified consumers and we have the data from mystery shopping on that.

So a couple things. I've got a forecast in here of mobile banking adoption. We're bullish on it and a couple of years of actuals. We look at consumers. We don't want to overlook the fact that the majority of consumers are not yet doing mobile banking and getting any

kind of alerts and so we have a tremendous amount of work to do. And a lot of them simply don't see the value. They have several stages of new technologies to adopt to get there.

Underserved people, as I mentioned earlier, are a tremendous opportunity and this is where financial services can really be this win-win of helping people get more control of their financial lives. Literally, I think, everybody wins except for unscrupulous businesses and criminals as we do this if we do it right. And by that I mean I see people paying more fees and feeling good about it because they're moved closer to their financial goals.

What mobile finance features are top financial institutions offering? We have about 15 here that we recommend as being the highest priority. We divide them up on the left as being among mobile monitoring, simple monitoring, money movements, which has a different set of security and infrastructure implications to advanced capabilities down here from bilingual to viewing rates and two-way alerts and unique enrollment in banking. You know, as soon as they come out with these charts, somebody will make it obsolete by offering new products so somebody has some of this now. But you'll see there's a great difference which says there's a lot room, had a lot of runway if you will and a lot of take-off room for providers to roll out new features.

The mobile channel from a security standpoint, I'm going to say something that probably will be a little controversial and if anybody wants to question, you know, what the details are, where we get them from, happy to take any of that as we have time for questions but this represents the downside of a particular channel and there's about eight or nine major channels from branches to mobile to online, ATM, whatever. The red is the downside roughly comparing mobile, online, the Internet, voice then I think we could show them all up here but for simplicity we didn't.

And the upside, how much can we improve somebody's security? And what we see here is that as we've analyzed a variety of features, they're actually -- we believe -- more security advantages available. We're not necessarily predicting how quickly they'll get rolled out but the technology exists today, number one, and consumers have shown us motivation, number two. So we think we can improve security through mobile but, of course, we have to do it right. As we look at the outlook, you know, there's so many ways, I mentioned before, if you get a picture half right four times in a row, you're six percent right after just that many iterations.

So how do we get ourselves to mobile payments and make a lot of money for honest people and scrupulous businesses and strengthen the economy, and protect consumers, all those good things? We think the technology to watch is review and release alerts. We're not pretending that there are not significant changes in core banking systems and business models and significant security concerns. All those loom large, but we believe that today to go from mobile banking, showing high penetration among segments to eventually where you leave your wallet or purse at home and you just don't even mind. You say, I guess I don't need that any more. We think the review and release alerts are the

technology to watch and I’m glad to be part of a group that includes policy makers because that’s the key to be able to do that right.

[end of transcript]