RAW FILE

ITU‑T

GENEVA, SWITZERLAND

4 DECEMBER 2019

FIGI SECURITY CLINIC: SECURING THE INFRASTRUCTURE AND APPLICATIONS FOR DIGITAL FINANCIAL SERVICES

1615 CET

Services provided by:

Caption First, Inc.

P.O. Box Monument, CO 80132

800‑825‑5234

Www.CaptionFirst.com

\*\*\*

This text is being provided in a rough draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. This text, document, or file is not to be distributed or used in any way that may violate copyright law.

\*\*\*

>> Blockchain is just dumb in some respects, even time and date is an Oracle. It's fit in, it's now says it's Wednesday. So if that's hacked, you have got problems. Crypto exchanges and user wallets, per security, now, crypto changes are sort of a one size fits all thing, they are meant to be the broken dealer, they are meant to change, they are meant to be custodians of private keys and some of them do it, but at lot of them are not doing it well.

So the honey pot is full for hackers to come in and steal, steal crypto assets, crypto coins primarily. User wallets are often pure security. So crypto exchanges I would highlight as one of the main effects of poor security, but not because of the decentralized nature, per se, of a Blockchain, it's because whether they work with decentralized assets, they are not decentralized in themselves. Crypto occurrences are in effect decentralized and act as a honey pot for hackers.

To as I said, there is no DLT protocols, they are testing varying initial designs with complex logs. And as I have seen mentoring a lot of these startups, a lot of startups without resources to assess and address security issues. Okay. I think I have got two nor slides. So some recommendation in the report, it's for policy makers, could develop or even mandate principles rather than specific technologies or standards. Security audits could be mandatory. Use of 12 factor authentication methodologies is available.

So here is one if you are Developing a DLT in the Developing world context, there is some design principles and how to go about it. So design who would set up and maintain security. These are questions that need to be asked if you are, say, an NGO, and you want to implement a Blockchain, these are the kind of questions I would suggest you ask. Fat the system level, how would you ensure that the vulnerable data was protected and at the individual level would you ensure that individuals could ‑‑ lots of text here, I encourage you, I am highlighting it and I encourage you to go look at it in the report. So that's it for me for now, so, again, follow me on Twitter and you will see all of these wonderful issues popping up every day.

(Applause).

>> MODERATOR: Thank you, Leon. I hope that we have some time perhaps in the conversation that follows to dig more into the questions and recommendations you have for how Developing country users of DLT or regulators of that can think about security and that very last slide. We are going to turn to Anne‑Sophie Cartray, but before we do, I wanted to ask a quick question, and hopefully a quick answer, but I was struck by the fairly long laundry list of risk areas across so many factors that you just laid out on those multiple slides, and wondering whether the paper that's been published makes any sort of assessment of the probability of the incidences and consequences of the various risk factors. That's such a long list. Is there a top three we need to be most concerned about or did we need to be concerned about every single thing you put on there. Some less likely to happen than others. I'm wondering how we are supposed to wrap our heads around how to prioritize what to do.

>> LEON PERLMAN: If you want to see it from a customer perspective rather than enterprise perspective ‑‑ let's take customer perspective because that's the most proximate class. I would say crypto wallets, if you are playing in that space, and people are, because it's not just about crypt though currencies anymore, it's about tokens, so we have evolved to what's called a token economy, we tokenize everything. I can tokenize this and I can tokenize royalties. The guest fees, the payment tokens. Everything is a token, but tradeable. So you are not trading crypto currency, you are trading components of the crypto economy and that storage is vulnerable.

So that's an immediate fix. I mean the efforts need to be concentrated on that and security audits need to be done, I think regulators can have a big role to play in that. Again, this is ‑‑ the other issue, and I will tackle this in some other writings is that the rule regulators don't know that they even need to do this, but that to me is the most proximate form of loss and vulnerability causing customer loss.

>> MODERATOR: Let's turn to our panelist who will share more about their own work and their reflections on the paper as well.

>> ANNE-SOPHIE CARTRAY: Thank you very much, Jamie and thanks Leon for this good overview of your paper. So what I'm going to do actually I have a few slides which are I assume try speaking about the key enablers who move towards new financial services infrastructure and looking at one example of the project we have been working on a consensus which is project I to I which was Developed in the Philippines and which is around payments.

Maybe not everyone is aware, we are a global organisation, we started as a startup, and right now we are 1,000 people globally, most in the U.S. and also across the rest of the world. And we are gearing towards Developing Blockchain solutions, enterprises and we are also part of the Blockchain for social impact so looking at what are the value drivers. When speaking about Blockchain and financial services, what are we expecting? The first one which is around operational efficiency, I mean, we often per see Blockchain and this is actually one source of truth, so it's to share the database among different markets participate in terms of financial services and there is definitely a lot of potential to reduce the number of consideration, is disputes, so on, so forth and to increase operational efficiency and to reduce the cost, I would say mitigating risks.

One of the variant stages is do an atomic swap when exchanging digital token or security and cash Document within the same leg, you know, so it’s a bit like all or nothing so this way we can really reduce the risk within financial services and then also transaction efficiency by kind of clearing and settling transaction in a much more efficient manner, transparency, capital efficiency, I mean, I think these are kind of the main aspects, but basically there are a lot of promises in terms of Blockchain, but then the question is how do we get there. What are really the key enablers to get there, and how can we build this market infrastructure or this financial services infrastructure?

So of course, as a building block these are Blockchains. Maybe I'm not so agnostic because we are working on ECIM, but it's a building block or the back hand actually is Blockchain. This core component actually included the cache or digital cache because let's say even if you want to tokenize an asset you need actually to exchange this asset cash, and if you want to utilize fully the potential advantage of the Blockchain, you need to have the cash also on the Blockchain which is often what we call as a stable coin even though there are different forms of stable coins but the idea is to have a representation of the currency, back devices, back currency on the Blockchain.

So I would say so cash is one important piece, one of the building blocks that you need in order to build your applications. Centralized identity or digital identity. We spoke about it in the previous panel, and also asset tokenization which is representation of the asset you want to exchange on the platform which is different than cash.

So make diving, diving into one project so I meant i2i I'm not sure all are familiar with this project. What's interesting in the Philippines is that it's a country of more than 100 million, I think, inhabitants, and more than two‑thirds of the population bank. And one challenge is they are dispatched in more than 7,000 islands. There are lots of people living on fishing on these islands so domestics and our bank network is really poor.

So for people to send money from one island to another island it's practically impossible or it takes a lot of time and it's very costly. So on this project we work essentially with Union bank, and the idea was to build a domestic remittance system. So what we have done is we worked with local branches, I think close to 200, I think 160 branches on this platform, and we work with them to build a network so it's, it's a private Blockchain, it's a private neck work. We ‑‑ network. We build the network where essentially someone on the island can go to a branch, bring the cash, and the cash will not only be put in an account which will be then transferred to another one and so on, so forth, which takes time, but it will be actually digitalized so it will be transformed into a token and this token then can be transferred almost real time. I think it's a matter of a couple of minutes to someone else on another island to someone else in the Philippines.

So I think it's an example which is quite interesting because here we have managed to bring it to production, so right now it's live actually for a certain number of branches in the Philippines and the idea is we need to build this network and provide actually payment services or remittancy services to unbanked and to provide them a service which is actually quite cheap and which is also like very fast because it's almost real time.

So maybe when we look at this project, coming back to what Leon was mentioning here in terms of security, like what have we done, you know, in terms of security. I mean, I'm not going to cover all of the regular, you know, treaty points, but there are definitely two which are very important. One which is around governance, which is essentially, so here we are operating within a private network. So private Blockchain, which is built out of Calico which allows enterprises to develop the quite quickly. So the first is define governance around who has access to what. I think it's a common problem around all types of Blockchain solutions whether they are public or private.

So currency is one of them and then security audit. So like for instance here within consensus we have, we have an audit arm I would say, a security audit time which is called consensus Rejoined and they have Developed a product MythX. So the problem is not now just to do an audit before you go into production, but to also embed your security audit throughout the development cycle of your platform.

This withdraw you can see spell check. If you are a developer, we will have this tool which is a plug in in the development platform and use it really as a spell check to make sure that it will spot vulnerabilities quite early on so it doesn't become something which would require additional fixing later on.

So I think this type of practice actually, you know, maybe will become more prevalent to ensure that we have robust, you know, platforms which have been built, and I think it's especially important because when you think of a digital kind or a kind which is on a Blockchain, this kind of benefit from all of the smart contracts properties. So you can essentially program, you know, this kind to do a certain number of things.

So it's really important actually to make sure this is done right from the get‑go and not wait actually for too long actually to correct it. So I think that's pretty much. I had a few videos, but I don't think we will have the time. Maybe I will just pass it on to the next speaker.

(Applause).

>> MODERATOR: Since I have started the question immediately after I will give the same courtesy to everyone. So before we immediate to Adrian. Just thinking about your experience in the Philippines and what we have heard from earlier panels and what Leon was saying about security taking a backseat to growth and really only action in understanding is coming when something goes wrong, the market participants that you are working with in the Philippines within the financial services ecosystem, were they worried at all when it comes to security and privacy of the solution that you brought, and if so, what were they worried about? If not, how does you bring that to them?

>> ANNE-SOPHIE CARTRAY: I think not only in the Philippine but overall, what I see is people are worried and maybe what Leon was mentioning is definitely true when it comes to start up, public Blockchain and all of that. As we are trying to evolve financial services infrastructure, whether it's in emerging countries or here, you know, like in Europe, there is definitely a lot of scrutiny around security and privacy. And I think it's maybe one of the maybe blocker to some degree of faster evolution of these types of infrastructure. Because I think right now we have at least in Developed Countries very regulated financial institutions. There are a lot of scrutiny about whatever happens in cases with situation or who is going to take the responsibility in case of fraud, and I think this question come up as we are implementing such solutions and people want to know, you know, and when you work with Union bank or Visa exchange or any other regulated entity, irrespective of jurisdiction, I think there are lots of questions which are being asked in terms of governance, in terms of responsibility and liability, and I think it's unavoidable, and I think we need to be able to respond to this question. I hope I responded to your question.

>> MODERATOR: Thank you. You did. We will move on.

>> ADRIAN HOPE-BAILIE: Okay. Can you all hear me okay. Thanks for having me, my first time here. I prepared these slides not knowing really what to expect, so I hope it all comes together. A little bit about myself and any background just to provide context on the journey and what I will talk to you about. So I have been involved in a number of companies with quite different perspectives on not only payments but also technology from Dot Mobi which was a consortium promoting noble Internet, ACI who is a vendor of payment systems that probably a lot of you know, Paycorp is a payment service providers providing ATMs, point of sales those things so I came from traditional payment world, retail payments and then joined Ripple where it was three years it had distribute ledger technology and solving payment problems using this fantastic new technology.

The last year and a half I have been at Coil, and at Coil we are mostly focused on the Web and micro payments on the Web and content monetization. So you are wondering why the hell am I here, but that's mostly because of the work we have done at Ripple that we continued to do at Coil in the Mojaloop project in collaboration with the Gates Foundation. I also participated in a number of technical standards bodies. I Co‑Chaired the payments Working Group at W3C and we have presented some of our work as IETF.

When I joined Ripple and it's still the case, the division at the company was ‑‑ the vision at the company was the concept of Internet of values. It wasn't that we have a DLT, what can we do with it. It was about how do we make money move as frequently as information does on the Internet. And the driver there, the reason for that analogy was looking at the Internet and looking at how it had democratized things like information so how do we take that and apply it to finance.

And our realization was that one of the major challenges we have in payments and especially in retail payments is fragmentation. And what fragmentation causes is friction. So one of the challenges if you look at something like the Internet versus payments networks is that the Internet is a single global network that, you know, there is this layer of interoperability. How are we going to solve that using the technology at our disposal.

What actually happened was while I was at Ripple is we realized as incredible as the technology is, it wasn't the panacea, the silver bullet that was going to solve interoperability. Blockchains don't give you interoperability. There are many Blockchains. So I think this has come up already today, if I'm using one Blockchain and you are using a different one, we are not interoperable. And so by necessity, there is a need to introduce what Leon referred to as these layer 2 solutions. And we have started to think of as simply part of the clearing layer. So if you think about retail payments and how they fit together, there is a layer of technologies there that are required to do, to take retail payments through its lifecycle.

You need to discover how you interact with the account holding entity on the other end of the payment. You need to set up the payment. You need to have information that's exchanged between those two entities to determine how much is being transferred and under what conditions, why, what information needs to be exchanged. Then you need authorization from the owner of the sending account to actually release the payment, then the clear the payment and you cycle it.

The reality is distributed ledger technology fits really well in the bottom liar but not as well in the layers above. So over the last few years, we have been exploring how we solve for some of those layers above on top of some of these new layers that we are starting to develop below. And so interestingly enough, about I want to say three or four years ago, we started engaging with the Gates Foundation on how do we help them to build a, build technology that reflects the level one principles? What would a reference architecture for a domestic payment system look like if you wanted to help promote interoperability.

Ultimately interoperability is what promotes competition and brings down cost. So the recognition from the Gates Foundation was that the way to improve financial inclusion was as simple as improving interoperability. And so what was tinting the initial conversations were how do we Ripple's distributed ledger technology to do that. And that quickly evolved into how do we use the interledger protocol, the clearing protocol to do that, and over time that's evolved and we are where we are today with the Mojaloop project which was someone who comes from traditional retail payments is an open source payment switch. It's open source technology so it's intended to bring down the cost of implementation for people who want to do it, but it's a switch.

It's clearing accounts for participating entities. It produces settlement reports that get settled by the central bank. And I think if, you know, for many of the people that have engaged with the Gates Foundation on trying to solve financial inclusion within their countries and have looked at the options available to them, and have assessed specifically the problems they want to solve, a simple clearing switch that can be implemented and run at low cost generally is much simpler to do, and as a result generally more secure as well.

So short and sweet from my side, looking forward to the Q and A, but there are some links to some of the work we are involved in.

(Applause).

>> MODERATOR: Thank you, Adrian. Before we open up to Matthew who is hopefully still with us on the line, I would love to, since you have been involved in Mojaloop and its development for too long I would love to hear a little bit more from you around the payments use cases that you think are going to be best served by DLT, and what has been, what's been on top of mind as Mojaloop has been Developed for a tool for financial inclusion and how we are actually thinking about using the technology to improve financial inclusion with respect to payments?

>> ADRIAN HOPE-BAILIE: So I think one thing that the foundation did which was, you know, was great in terms of trying to solve the problem was they did a huge amount of research up front and identified specifically what were the things they could do to address financial inclusion, and they weren't naive to the technologies that were available. So they looked at DLT very critically and I think they realized and certainly this is my opinion as well, that it has a place, but it's very immature, and most likely the place for DLT will be in wholesale payments.

So it will be something that's used maybe right in the tight knit circle of central banks and commercial banks. We are talking now about in the realm of feared currency. Obviously there are use cases and other ways you can use LDT. The realization with Mojaloop was the realization that we need to building on top of that. The specific problem they were trying to solve was we have a whole lot of mobile money operators out there, explosive growth, fantastic way to bring people into the digital financial services ecosystem, but they are not interoperable, so there is very little competition and so people are holding three SIM cards to be able to transact with people on other networks, so on.

So by simply pulling all of those players together, making them interoperable and promoting competition in each of those markets that was suffer to be driving the level one goals and that DLT really didn't have a specific role to play there.

>> MODERATOR: Thank you. Hopefully we will have more time to discuss later. Let's turn to Matthew Davie who will take us back to Sierra Leone and the Blockchain digital project there.

>> MATTHEW DAVIE: Awesome. Can you hear me? Okay. I will assume you can hear me. Okay. I will start going. So I just wanted to take something Leon said early on on his slides which is security equals technology and governance. I think we often get lost when we start talking about DLT, talking just about the technology side and Kiva and when I talk about Sierra Leon and I'm on the board of Libra, all of the hard work is at the intersection where technology meets governance and policy. So for financial inclusion, I don't have to beat the stats about the 1.7 billion adults that are excluded. Our thesis on the approach to get towards financial inclusion and to bring security and privacy to distributed ledger technology systems is a multistakeholder approach. It's the regulation financial policy plus the users, and the users, what they are chartered to do is privacy, consumer protection, KYC, MLFT, what disabilities today in terms of DLT is a capacity gap when you talk about the stakeholder of Government or regulators, you have to help build or provide them a pathway to build that regulatory and technology capacity.

With FSPs this has to integrate with existing systems. It doesn't work for a bank to say you are now transacting in bitcoin. Customers have deposits in dollars or Kenyan Schillings so you have to have the operability to settle up between multiple currencies and this doesn't gift for financial service providers especially for poor countries. And for the users, you are talking about 2020, and 2025 technology and they have 1985 technology today. So there is a digital education gap. There is a financial education gap that exists, and that has to be bridged.

So in Sierra Leon, that is the key example of looking at that entire multistakeholder approach and not saying we are looking for a place to apply DLT. We came to DLT because it's the best technical solution for the technical part of the problem, but chat leverage is there is no infrastructure for digital financial services.

The country wasn't ready for digital financial services let alone DLT. We worked with the regulator on how civil identity it issues how they want to regulate consumers and protection and help them build capacity for them to issue the digital credentials using the identifiers. With the financial service providers we worked with the central bank, we are still working with the central bank. For them to provide the integrations for KCYML compliance to every financial service provider in the country. Now, it's a small country, there is something like 28 financial service providers so this is not thousands of entities, but, again, solving that gap that exists for financial service providers working with their regulator to solve it.

So their identity verification and their credit reporting and they are KY CML compliance, like all of the stuff is provided with open source API integrations that allow them though integrate into their existing MIS systems. And then for the end users, it's all about making sure they can actually use it and they understand how they are using it, so there is a consumer protection and education portion of that working with Government regulators and CGAP and others to help that, there is also the acknowledging that people who are financially excluded don't have an iPhone or a great Smart Phone in their pocket to making sure how to use it, where to use it and buy to use it with the financial service providers.

>> So what this has done, and what will continue to do is making it so that those who couldn't pass an identity check can do it as easily as bringing their national ID card and a thumb print into any bank or any MFI agent so make it that any bank instead of not knowing somebody's credit history or knowing their identity for two seconds and it would cost 12‑cents you can get an identity verification that is a KYC check and pull a credit report and then for the Government building the capacity for them to regulate the system.

 I think it's important for DLT systems to be thinking about the regulators. That's on the Kiva side. Very quickly will make a comment about Libra. So I will maybe preempt a question, and Adrian was hitting on this when he was talking about Mojaloop and especially about Ripple, but moving money is hard, and when you talk about financial inclusion, once you have readiness for digital financial services, the next thing is actually moving money digitally. And the things that hard about Libra in my opinion is it's forcing ten years of regulator discussions to happen in ten months and that should be hard and it's important and I hope that has spillover effects for everyone because since Facebook is involved and Facebook has such big scale, you are talking about something that can't be ignored.

So it's forcing regulators to have discussions really quickly that may not have played out over the next decade and Libra is working at the intersection between the technology and the regulators. I think that's a very important thing because the regulators are the ones who are there. And when you talk about security, they are the ones who are elected, appointed and have the charter to go out and say this is how data moves, this is how money moves, this is how you can trust the system.

So I'll leave you with the future is here. It's not evenly distributed right now and I think we have the opportunity to change that, and the two examples I just gave with what we are doing in Sierra Leone to give DLT readiness and at a financial scale and what Libra is trying to push in terms of interoperability at a global scale are two examples of things trying to push both technology and regulators towards a future where the system can be more inclusive.

>> MODERATOR: Thank you, Matthew. And thanks for preempting what I'm sure are going to be a few questions on Libra and where that is headed. So just a quick question to you before we open it up more broadly, to Leon said, and you also reiterates that security equals tech plus governance, and then Leon listed at the end of his presentation a brief snapshot but of an extensive list of questions that need to be asked when deploying DLT technologies for financial inclusion. And yet I think what my core take away from what I just heard from you and throughout this panel are some of the huge capacity gaps for regulators not only in the Developing world, everywhere, to assess and address the security vulnerabilities of DLT.

So I would love it if you could tell us a little bit more about the experience in Sierra Leone. It's recent, it's still ongoing, tell us more about the issues that surface, the types of conversations that you and the partners that you have had to bring in hand with the regulators, what were the concerns that they had or that you felt like they needed to be more aware of and prepared for.

And if there are any specific recommendations that you would have for the people participants here in the room who maybe regulators are working with regulators for things they should be looking out for if they are considering something similar.

>> MATTHEW DAVIE: Great question. So first to come, I mean there are two things unique about Sierra Leone or unique about going to Developing world. If you go somewhere where there is no digital system, there is not an entrenched legacy system to try to move, and Sierra Leone is definitely one of those countries are, where there is a decent amount of mobile money penetration but digital financial services were not strong two years ago when we started working with Sierra Leone. So that's a huge blessing because you can actually look and white board with the Government, whether it's the central bank, whether it's the finance Minister, the head of state, and you can go through and blue sky it which is really nice because there is nothing holding you back.

So capacity gaps, so in Sierra Leone, you can do two things, most DLT in the past and most cryptocurrency have issued the Fiat system and said we are going to build our own garden over here, that's very fast but oftentimes has a hard time becoming compatible with a Fiat and a sovereign so sitting up front and working with them specifically on consumer protection around financial services is really important, and then privacy policies.

So the hacks I would give people is to sit down with usually it's the Minister of Interior affairs who controls identity, and then usually it's the Minister of Finance and central bank governor who controls economic and fiscal policy and half of the discussion up front to destigmatize it, because cryptocurrency has the stigma of bitcoin and how am I going to control the system? How will I provide assurances to citizens if I take such forward looking tack that it's privacy by design and everything doesn't come through my server sitting in my closet at the state house. How do I do that?

So sitting down up front and having the discussion, and that technology is part of the solution, but technology is not the solution. I think that's a really big one. In terms of building capacity, a lot of people assume that it's hard to build capacity in these places. It's not. There are a ton of people. A, the Government wants to build this capacity so that it can manage its own affairs and not be reliant on external parties especially when it comes to technology because of how fast it moves, but there is a shocking number. It shouldn't be shocking, but it's shocking until you figure it out. There are a shocking number of people who have gone from these countries and gone to M.I.T. and gotten Ph.D.'s who would love to go back and have the legacy be, I went back to my country and helped us be prepared to we didn't get steam rolled by the fourth industrial revolution.

So up front talking with the regulators and make sure you can help them extend policies to cover this so they have control over the system and then, second, making sure there is a pathway for sustainable incountry and especially technical capacity that you can get a country CTO and build a pipeline of technical talent to the country.

>> MODERATOR: Thank you for that, Matthew. This thing in the ear, when you speak is confusing. Awesome. I have asked a bunch of question. I have more, but I thought I would pause for a moment and look for a show of hands in the room of how many questions are there from the floor right now so that I can forego my time for others to be able to speak and have a conversation. I can see how many questions we have at the moment. Only one. Did we already discuss DLT extensively enough in the last session or is the coffee just not strong enough outside? I think there may be both of those. Is it too complex in we need to take it down a notch. I feel like I'm pressuring you now, but I am I little bit surprised.

I'm not starting until we have five questions in the room.

>> Maybe one about DLT and not about DLT.

>> MODERATOR: We have three questions and one is not about DLT, so that's that. So I'm going to ‑‑ I will ask a couple of questions and we will come back to you. So coming back to Leon, so I am curious about you earlier today showed a ‑‑ we talked a lot about the feature phones and how in someplace that's 75 percent of the market. Now, there are smarter phones, smart feature phones, and then the Smart Phones or coming down in price and becoming more prevalent, but curious about how those with feature phones which is a very large percentage of the market that we are trying to financially include, so how can those with the feature phones without the security built into them the way that other phones are participate in the crypto economy? Is there a big gap between what we have been talking about today and actually what is useful for the poor and excluded that we are trying to figure out how to include more?

>> LEON PERLMAN: That's a very good question, thank you, Jamie, feature phones even though they are made smarter will still be dumb. They don't have enough memory for the encryption and the like. You have got to see them not as participants unchained. You have got to see them pas offline oracle, as contribute. Any information they provide to a Blockchain, it's information paradox in Blockchain, what is put on a Blockchain isn't necessarily truly. That is the same thing you need to take into account with insecure Oracles. Feature phones can't participate. You have to realize that the information is not verified.

There are companies that are Smart Phones like HDC and the like coming out of Smart Phones that are unchecked, this is off check. There are some companies I have seen in the last few weeks have come up with solutions where you participate in a Blockchain. I haven't gotten into the nitty‑gritty of how they are doing it, but you access a Blockchain by SMS and USSD, and we have heard today that USSD is not exactly, you know about USSD.

So I think there is a role, and there is a need for a role, but these are seen as Oracles. The action is really at enterprise level. These are really just feeder mechanisms of the Blockchain. And Mr. Sharma and I, we discussed this a bit earlier that the action is really at the enterprise level, at the back end level.

>> MODERATOR: Thank you, Adrian, I wanted, so you gave a nice kind of background overview of Mojaloop, and we talked a lot about its intent but we didn't talk very much about security features or any of those concerns or worries. So I'm wanting to hear about what you have seen as potentially some of the security or privacy challenges with the interledger protocol or whatever else is used on the back end there of Mojaloop, and just what was most salient for you and the team when you were Developing or have been working with the team on deployment of Mojaloop?

>> ADRIAN HOPE‑BAILE: So the interledger protocol was the piece we had been working on at Ripple. Really it's a clearing protocol for curing payments between participants that doesn't necessarily have direct financial relationships. It's very simple and it uses very basic cryptography, just hashes.

A concept that's actually used in the lightning network, almost identical to how the lightning network works that Leon was talking about now. The difference being that it doesn't purport to try and report anything back to the settlement layer, that's not built into the protocol. So what Mojaloop did was they adopted the same concept. So what is it does is the every time you do a transfer of value, you create what we call a condition and the transfer of value is only considered committed at the clearing house if the recipient can provide the fulfillment of the condition. So it's a hash and a preimage for those who understand the cryptography.

So that's a small, very small step in improving traditional clearing protocols. If you look at, for example, how card networks worked to, they are completely insecure. Card networks are basically everything sent in the clear other than a pin block. They are like the SS7 networks, they are only secure because not everyone can get onto those networks and they operate privately.

So it's an improvement that way. And the other things that Intel is separate the block from the movement of the money. If you look at how a Mojaloop happens there is change between the two entities that we call the quoting phase and that's the time when you exchange data, determine how, you know, why the payment is happening, who is involved, what are the fees going to be, all of that stuff is determined up front. And then the actual transfer of value is really, really simple. It's, okay, based on this whole quote that we have just completed, now move the money.

And the commit from both parties has this cryptographic hash which provides quite a nice audit trail if you ever go back to the clear is house and want to verify that all of these things happen. Ultimately the goal is that you can connect many of these transfers together for a single transaction, and the same hash will follow through all legs of the transaction, and so you will be able to start connecting networks together, doing things like effects, adding third parties and have some level of cryptographic surety that the transaction went end to end in its entirety.

Beyond that the security is the standard network level security that we expect. Mojaloop does things like signing all messages, ensuring that participants find certificates for authentication. So it goes a little bit beyond what maybe traditional payments would have done with things like ISA222, it takes a step further it defines APIs, the messages but it also defines how the security should work between participants which I think is a very valuable addition to typical interoperability and payment standards.

>> MODERATOR: We will try again on the questions. It has to be someone who has not asked a question today. If.

>> AUDIENCE: Till ask the Libra question. This is for Matthew. You mention and I want to make sure I'm getting the sort of ordering combined. You mention that you are working with Governments to improve their comfort level with Blockchain technology. And so the thing that jumps to my mind is that there is bitcoin and there is Libra and Facebook doesn't really have a track record that promotes confidence, and also the it U.S. doesn't have strong privacy protections.

 I'm curious practically what do you think the board can do, and how, as, well, if I were a user of the system, how can I be confident that there will be standards compliant, they will protect my privacy, you know, what sort of measures do you think can reasonably be done.

>> MATTHEW DAVIE: I think two broad comments on Libra, one is just to make sure everybody understands is Libra was born out of Facebook but it is not Facebook. It is an independent association in Switzerland that has a board and the only governance Facebook has is David Markus who has the co‑Libra which is Facebook's wallet for Libra. He is on the board with me. And they have one of the 21 votes at the Council level.

To it's a permission network run by currently 21, we will probably scale it up to 100. Here is the catch 22 on Facebook, I would tend to agree their recent track record the last couple of years on consumer protection and privacy has not been great. But the other side is if you go to the Developing world and you go to the unbanked world, for 90 plus percent of people, they get access to the Internet, they get access to a Smart Phone, and they install a Facebook product, usually it's WhatsApp, sometimes it's messenger.

So here is the catch 22. If you do want to solve for a big global problem like global financial inclusion, and you identify technology can be part of the solution, and Libra is an expression of technology as part of a solution, don't tell me, and this is me speaking as Matthew from Kiva don't tell me you can solve that without Facebook because Facebook touches 2.4 billion people and they own well willingly touch people who are recently included digitally. So if you want to get towards that tip of the spear and get towards the last person you want to include, it's important to have Facebook at the table.

Baking protections in, I don't think technology is the right place to do it. I think there are a lot of things you can do with technology to build trust into the system and you should do as many as possible, but in my opinion the most important thing is what is the most publicly, looks like the most painful things which is having discussions with FINMA and with The Fed and with BIS and all of the institutions to arbitrate the trust in the financial sector in consumer protection and compliance, and Libra is doing those things head on.

And that's not easy. It would have been much easier in my opinion for Facebook to have just gone and done a bunch of Blockchain and crypto currency under the hood of Facebook pay. What is very important is they opened this up so that every user that Facebook would add to the crypto currency platform actually could move to another vendor, could transact not through Facebook, and I think this is a huge win for humanity, because if you go back 15 years everybody has been doing things in silos, when I look at Libra, I look at Facebook saying, you are right, I could have done this myself, but I am contributing to the open source and opening it up to this other permission network of people and I want to make this so we are globally interoperable.

I personally think that should be applauded because they didn't have to do it and as KIVA operating in 94 countries around the world, Facebook being part of the solution is super-duper important. So I hope that kind of answered the question.

>> MODERATOR: Wonderful. So we just have a few minutes left. What I want to do for our wrap-up, taking a comment that I heard just a few moments ago about how this was quite technical and maybe perhaps a little too technical to generate the kind of conversation that I think we had hoped to have.

What I would like to do is close us with a round from, comment from each of the panelists where you say in the most layman terms that you can conjure in these very technical conversations, your one-off promised and peril dichotomy, one hope and one fear when it comes to the use of DLT for financial services, just one of each and you will each have about a minute for a closing remark. And I think maybe we should start with Matthew since you are already on the line and had the floor, so continue, please, and then we will close with those in the room.

>> MATTHEW DAVIE: Yes. My hope and my fear are two sides of the same coin, which is digitization is rapidly happening and it is impacting mostly vulnerable populations who have not been digitally included. And my fear is that we miss the opportunity over the next five to ten years to put humans in the middle of the technology, and DLT and decentralized technologies whether it's identity, credit reporting, central bank digital currencies are an opportunity to give agency and give power to the individuals by design and by default.

And so my hope is that as many places as possible we do that, that we put human beings in control of their data, in control of their transactions and extend the financial sector so it can include them and extend regulations to operate that way. My fear is we won't. My fear is we will end up with a way to use crypto currency to buy a blue bottle cough any in Manhattan and there will still be a billion people making less than two dollars a day.

>> MODERATOR: Thank you Matthew. And we turn to you Sophie.

>> ANNE-SOPHIE CARTRAY: It was really well said by Matthew but I will not say the same thing. I think to me, it is balanced to find between technology and humanity. I think it's important. I think it's also important for the entire ecosystem to move, because I think at the end of the day, these types of solution when we speak about DLT, it's all about sharing data or information or infrastructure.

So I really hope actually that we will be able to, as an industry, as a role and globally to evolve this infrastructure together and so on the legal side, regulatory side, we can move in the same, you know, like that we can evolve at the same time. So I think it's my hope, no, and the risk is that we keep on moving, you know, in silo, and that we don't go anywhere, because at the end of the day, it's an entire ecosystem which needs to move and not just kind of one piece of it.

>> ADRIAN HOPE‑BAILE: So I guess when approaching any problem, my hope is that people will think about the problem they are trying to solve and not how they can apply this cool new technology to the problem. So think about specifically what it is they are trying to achieve and goals, and I think in many cases we are talking about the entities, we are talking about our central authorities, sings like central banks, and so using a technology that's designed to operate when you don't have or need a central authority is exactly the wrong time to use it.

So my hope is that those regulators, those entities concentrate more on creating regulation that fosters competition and innovation and allows others to deploy distributed technology effectively, and my fear is that they will spend too much time trying to deploy it themselves.

>> LEON PERLMAN: A lot of it has been said, so,, so I couple of touch points that I would agree with, silos, for example, my hope is that the crypt economy grows. It has the potential to democratize finance at a more accelerated pace that I can say digital financial services because it allows you to go across borders, a token economy allows you to get fractional ownership of many, many, many things. You don't have that now.

But you need, you need everybody to speak the same language, not sigh lows, so the silos, again, this is both sides of the same coin. The silos are in a fragmentation. We are not going to get there if there are a thousand different ways of doing the same thing. It's just not going to work. And there is no interoperability. Silos also between innovators, those in the crypto industry if you want to call it that and regulators. I do a lot of capacity building and I still see the silos where bitcoin equals Blockchain equals drug money. Still, believe it or not, that ethos permeating the regulatory world, although that is changing. There is a lot of capacity building going on, but that will happen when industry and regulators get together.

And in sand boxes, perhaps, so less silos, less fragmentation, and more decentralized finance and which will lead to more financial inclusion.

>> MODERATOR: Thank you very much. I think we are now at the end of our time, so if you would please join me in thanking our panel for their contributions today and thank you, Matthew for sticking with us. I believe that we are moving straight into the final session if you can believe it, the day is not done. We have more to go and a cocktail reception. So after a glass of wine you will have more questions about DLT that you will want to corner this team on to ask a bit more.

Thank you very much, and I'm sure someone else will be coming to tell you what is happening.

>> MODERATOR: Good afternoon, everybody. We have an exciting panelist discussion and since we are last we can say we saved the best for last. So thank you for all sticking with us in the last session, my name is Amy Ulrich I work for KCS health. My colleague Abby presented on authentication today. I do want to introduce panelists here starting from my right, we have Rehan Masood, he is from the state bank of Pakistan, we have Dorothee Delort from The World Bank, Vijay Mauree when you have been introduced already to with the ITU, Kevin Butler with the University of Florida, and then on the phone remote hopefully, we have Dalit Caspi‑Schachner and she is from the bank Hapoalim.

So for the session we will give an overview of the security assurance framework report. Hopefully you had a chance to read it. If not, you can read the 60 some page later. We will start by reviewing threats and vulnerabilities from DFS, provide a framework for risk management and hear real life examples for how the frameworks have been implemented and how they have handled risk.

We are going to go a little bit out of order. We have one of our panelists who has a time constraint, so I will first like to invite Dorothee Delort to give a quick introduction and present some slides.

>> DOROTHEE DELORT: Thank you very much, Amy. Yes, I apologize, I need to leave at 6:00 and Vijay and Kevin were kind enough to accept that we swipe the order of our presentation. I would like to speak to you today about the cyber resilience for financial infrastructure that has been done under the Fiji security Working Group and go back to some terminology by financial market infrastructures, we mean payment system and also security settlement system, but today we will focus on payment system because payment systems are a critical foundation for digital payments and digital financial services.

They are the system where in the end transactions will be cleared and settled. And many studies have been conducted and I think the latest one from the IMF demonstrated that financial market infrastructures concentrate risks and especially cyber risk. And we felt that there was a need to look into that more in depth.

So cybersecurity and cyber resilience for financial market infrastructures, what exactly do we mean? It's a very dynamic context where the scope of each activity continuously changes, so from ‑‑ we have risk management, information security, business continuity, information technology, and then cybersecurity. And we think that it's very important not to stick too much to the definitions, but to look at the purpose and the rationale behind security measures.

So here in that space, we will really look at cybersecurity for financial market infrastructures. So these financial market infrastructures, they tend to follow standards and best practices that are set up by the CPMI, which is the Committee for payment and market infrastructures of the bis located not far away from here in Basal. So the CPMI and the IOSCO for security settlement system have issues over the years a number ever principles that are the basically the key principles on which a payment system should be built in order to be safe and efficient.

So in 2012 following the 2008 crisis, the CPMI‑IOSCO published infrastructure for financial markets which are the book, the Bible or whatever your book is, this is the book for payment systems, reviewing all risk and making proposition on how to manage risk. There is a principle on operational risk, principle 17, but it was a bit limited on cyber risk so the CPMI‑IOSCO on cyber risk and cyber resilience for financial market infrastructure. And this guidance is structured into five main risk management categories, and three general components.

So you will know most of them, the innovation that came from this guidance from the CPMI was governance, and governance being at the centre. Because identification, protection, detection, recovery, you can already find them in the framework, for example, but governance being at the center was really the innovation in the CPMI‑IOSCO guidance.

And then there are three general components test, situational awareness and learning and evolution. But then the question that we, or the problem that we faced in many of the countries where we work is that the central bank would come to us and say this is very nice, but this is also very generic, very high level. How do I implement this? How do I operationalize this guidance in order to make sure that my financial market infrastructure, the foundation for my digital payments, my digital financial services are cyber resilient.

So the Working Group, the work stream on cyber resilience for FMI set out to identify adequate tools in order to operationalize the CPMI‑IOSCO guidance, and in that work, we Developed a collaboration with the European if central bank and realized that the European Central Bank methodology so cyberspace oversight expectation was the perfect tool to operationalize the CPMI‑IOSCO cyber resilience guidance and that this methodology could be used far beyond the system, but for all of the central banks operating a payment system basically.

And even for FMI, private sector FMI operating a payment system, because of these, so cyber resilience oversight expectation, CROE for sure, set up a more detailed elaboration of the guidance and they really are a detailed guide on how to go about those five elements, five components and three overarching elements. They provide and released good practices which can be referred to when assessing an FMI and when as a regulator giving feedback to an FMI operator. And what is really nice especially for industry and private second is that these CROE they take into consideration the very best practices already set out in different frameworks such as the Nist framework, KRcobit, Iso, all of these best practices are used and referred to in the CROE methodology. It can be used by the system operator themself to self-assess. It we do we think it can be used in any country and whatever the sophistication of the systems did because there are three levels of expectation starting from the most basic level which is called evolving to a medium level of sophistication which could be called advancing and to very highly sophisticated system we are talking the target 2 in Europe or the fed wire in the U.S., for example, that are innovating, and you see that it always in innovating, advancing, evolving because this is an every changing landscape.

So you can't be a one and done. So, and you have to adapt to the changing environment. I'm sorry. So what are, again, the three level approach. So an evolving system would be a system where essential capabilities are established and sustained across the FMI to identify, manage and mitigate cyber risk, and all payment systems have to meet this basic or entry level. The advancing level is a system where practice incorporate more advanced implementations that have been improved over time and where capabilities are harmonized across FMI. The last level, the innovating level, is really a level where the system, the FMI itself will not only look at itself, but also contribute the cyber resilience of its participants and the overall ecosystem.

So now, I'm going to be very quick in giving you an overview of what is in the CROE so in the CROE for each of the three levels, you will find a number of a list of topics that should be covered under each of these five elements and three component and three overarching elements. So the first chapter on governance, it will really refer to the arrangement NFMI has to put in place to establish, implement and review its approach to managing cyber risk. It will start with a very clear and comprehensive cyber resilience framework, and the framework should be guided by the FMI cyber resilience strategy.

So for each of these elements, the framework, the cyber resilience strategy, the CROE will offer a number of or list a number of topics that should be covered. So this is a very detailed and specific methodology. It will also cover the roles and responsibility of the board because for a very long time, especially in payment systems, but cybersecurity was seen as something for the IT people, something for even the ITD department.

And it has to be clear that cybersecurity, cyber resilience is something for the board itself. We have very direct reporting line to the board, and also appropriate resource and expertise that have to be allocated by the board in order to implement. So in the governance chapter will be covered the cyber resilience strategy and how to build it, what it should cover, the cyber resilience framework, processes, people, and resources, the role of the board and senior management, and culture, skills and accountability.

So this will be covered in the governance chapter. The identification chapter will, for identification it's crucial that FMI identify which other operation and supporting information assets should and in order of priority be protected against compromise. So really the ability of the payment system to understand its own internal situation as well as external dependencies is critical for identification. So it will require that an FMI knows it's information assets and understand its own process, procedures, systems and dependencies.

And so in protection is the chapter that is the more detailed in providing guidance on how the FMI should implement appropriate and effective measures in line with a leading cyber resilience and cybersecurity practices, and this is at chapter where you will find a lot of reference to industry standards and best practices and it will cover protection of processes and assets, control implementation and design, network and infrastructure management, logical and physical security management, change and patch management, people management, human resources security, security awareness and training and supplier and third party security management, which is also critical.

In the chapter on detection will outline monitoring and process‑related guidance aimed at helping FMI detect cyber incidence. And in the response and recovery, it will detail how FMI arrangements should be designed to enable it to resume critical operation rapidly, safely and with accurate data. And it will cover cyber resilient incident management, date security, collaboration, contagion, crisis communication and responsible disclosure and forensic readiness.

So these are really the core of the engine, but I think we should not forget that testing is an integral component of any cyber resilience framework for a payment system, and so the CROE gives guidance on how to conduct vulnerability assessment penetration tests, and even for more advance system red team testing on situational awareness, this is where you have all of the recommendation on cyber threaten tell against and information sharing, which is also critical and which is an area where we see a lot of need for guidance on information sharing, how do I go about setting up information sharing for my country. The last one is learning and evolving because as we said continued cyber resilience amid a changing threat environment requiring to continuously change. So key messages, a need to continuously monitoring on trends in cyber-attack, focus not only on technology, but also processes and people, and I would like to say that there are already some countries that following the work of the Fiji work stream have decided to use this methodology to assess their system and we had original workshop in Latin America in order to disseminate this methodology and most central banks from a Latin, Caribbean, Mexico, Argentina, Costa Rica, Colombia, basically all of them, and several central banks have already announced that they intend to use this methodology to assess their own system, their system that they operate, but also they will request operators that operate payment systems to use this methodology to assess their level of cyber readiness and to improve their cyber resilience.

Thank you.

(Applause).

>> MODERATOR: I know you have to leave, but before you leave, I want to get one question out of you if you don't mind. You mentioned CPMI‑IOSCO guidance states that testing is an component of any cyber resilience. Can you give us an idea on how testing can be done on financial market infrastructure.

>> DOROTHEE DELORT: That is a key aspect because all elements of framework should be rigorously tested to check overall effectiveness before being deployed by the FMI itself, and they should be tested regularly after, and this includes the extent to which the framework is implemented correctly, operating as intended and producing the desired outcome. So sound testing regime produced findings that are used to identify gaps, and the analysis of testing results provide direction on how to correct weakness or deficiencies in the cyber resilience posture.

So vulnerability assessment that is done by external parties is one such as a penetration testing, so a regulator can request that an operator of a payment system produce on a regular basis penetration tests that have been produced by third parties. And for the most advanced system, the red team, test team and ethical red test team, it's also very useful and, for example, in Europe most central banks are now moving to red testing on the live production, because you have to differentiate the test, and the tests that are produced but not on the live system from the red testing that is produced on the live system without advanced notice, but by teams that are ethically trained.

Because, of course, we would not want these vulnerabilities that have been identified to be then sold to people that might not be.

>> MODERATOR: Thank you. Will.

>> AUDIENCE: Just a very short one if I may.

>> MODERATOR: We will save questions for the end.

>> AUDIENCE: It was just to thank her for putting back the security Tempo shove I say to be neutral in the centre of the village. So thank you very much.

>> MODERATOR: Thank you. Next we will move to Vijay Mauree and Kevin Butler who will produce the security information part on Security Assurance Framework.

>> VIJAY MAUREE: So both Kevin and myself will present the report of the security Working Group on the DFS Security Assurance Framework. So it will be a joint presentation. I will start first and then I will hand over to Kevin to conclude the presentation.

So the report I'm also going to cover also a bit how it complements the CROE methodology that has been presented by Dorothee. So what's the motivation behind the DFS Security Assurance Framework. The main reason has been basically because as I mentioned a bit this morning, the DFS ecosystem is really a complex ecosystem. As these entities, all of the entities in the ecosystem are interconnected. Basically the security boundaries are extended. There is reliance on numerous parties for service delivery, and the mobile ecosystem itself is increasingly complex. There are a number of devices that have to be supported, different versions of operating systems each with their own vulnerabilities in how to be managed.

So the questions that we posed ourselves were what are the security threats and what are the control measures for stakeholders within the DFS ecosystem. When we look at these security threats and control measures we focus mainly on the telecoms infrastructure, the DFS applications whether they are based on Android, whether they are based on USSD or STK environments, and we look at the device security as well. Whether it's the mobile phone or the POS device, et cetera, and we focus mainly on those that are within the scope. So, for example, things that are under the payment service provider, they are already a number of, I would say regulations or best practices that are out there from the PCI DSS and other consortia. So we don't go into that. We basically recommend that these be adopted.

So the goals, what are the goals of the Security Assurance Framework? It's basically to bridge the knowledge gap and recommend a structured methodology for risk management. And the main goal is to basically enhance consumer trust and confidence in DFS, also clarify roles and responsibilities of each stakeholder in the ecosystem, and identify the threats and vulnerabilities at different levels within the ecosystem, develop security controls that will provide end‑to‑end security when implemented and also strengthen management practices with respect to security risk management in a man that is inclusive to all of the shareholders.

So in all, the security assurance framework is actually intended, you know, for all of these stakeholders, but principally to the ones that are involved on the side, that is the banks and non‑banks providing mobile money services, Mobile Network Operators and also technology services and third party providers. For payment system providers and merchants, there are already like I said before a number of let's say best practices or rooms or regulations that exist ‑‑ rules or regulations that exist already from the banks or, for example, the European Central Bank, OPCI, or Mastercard and Visa. With regard to regulators they can use the framework for establishing security baselines for DFS providers and then they can use these to basically audit DFS providers on the security posture.

This DFS Security Assurance Framework is based on the ITU‑T recommendation X.805 which identifies basically defines also what is a threat, what is a vulnerability, what is a risk. And we look at the threat, vulnerability and risk from a layered perspective looking at the application layer, the services layer, the network layer, and we look at the risk, the threat and vulnerabilities from these three layers perspective, and we also identify the recommendation identifies eight security dimensions with regards to the security control measures to address basically access control authentication, non‑repudiation, data confidentiality, communication security, data integrity, availability and privacy. These are the eight security dimensions, so basically all of our security control measures would fall under one of these eight security or some of the eight security dimensions.

Okay. When question analyze the threats and the vulnerabilities, we also consider the DFS provider business models. That is, for example, the bank led model where there it's the bank that performs the main financial roles and they make use of the mobile network operator for the communications with the DFS users. MNO‑led, where is MNO is the one that provides the communication, but also the bulk of the financial roles and also manages the DFS agent network. The other business model is the MVNO‑led, where here we have an MVNO services using an MVNO truck, and DFS is provided either with the bank or it’s an independent function and then we have a hybrid model where the roles are actually shared, critical roles are shared went the bank and MNO and third parties provide additional services like we may have a payment service provider in the ecosystem.

Now, why do we consider all of these business models is because we need to map out the threats and vulnerabilities within the ecosystem. So within each of these end system entities, we consider the risk and the threats and the vulnerabilities, and we look also at the different elements, how the service is actually being delivered. Here we have two, we have two elements that we will look at. The first one that is shown on the slide right now is DFS ecosystem for USSD, SMS, STK, or data transfer service provision, and here we have the user accessing the system with the mobile, with his mobile device, which may be a Smart Phone or a feature phone, and you can see it traces the path of the transaction from the user device until it reaches the, either the MNO or the banks. There are a number of third parties through which this goes through. So it goes through the mobile network base station, then the system within the mobile network operator and then it either is moved to the bank or to other DFS providers that deliver other services in the, to the user.

So all of these there are threats and vulnerabilities. And what are the threats and vulnerabilities? We will come to them later in the presentation. And then you have what we call the digital wallet DFS ecosystem where we talking about the Smart Phone application, no longer talking about feature phone here. So the device itself has a number of vulnerabilities. You have a wallet application with, that sits on the device OS that needs to communicate with the secure element, and then if it's based on NFC, there is also the NFC controller that is involved in, and the communication takes place either through 3G, 4G, WiFi or a code or NFC capability involved. So you have the mobile network operator, then have you mobile payment providers that provide the digital wallet, then you have the card issuers if they are also involved, and you have the payment network provider, those that provide the token services as well.

And this is actually a much more complex ecosystem, and we go, we explain this in more detail in the report. This gives you a scale of the complexity of managing the threats and the vulnerabilities. So the main components of the framework, if I can summarize, it has three main components. One is security risk management methodology, which is based on ISO, ISE2705 and that's in section 7 of the report ‑‑ 27000 of the report, we have the threats and vulnerabilities to the underlying of the mobile network operator the DFS provider, the DFS application services so this covers an assessment of the threats for this ecosystem and this one, which is covered in the report, and that's in, again, in section 8 of the report.

And for the threat analysis, we also have the security control measures for the different threats and vulnerabilities. And there are 117 security controls that are outlined in section 8 of the report. So this Security Assurance Framework, it provides a methodology for managing risk and it also has some security control measures for DFS ecosystem players. And these security control measures can be plugged straight into the security risk management program of the DFS provider.

So if you already have the security risk management program or they have a security management program, these control measures could fit in right there. So now I pass over to Kevin who is going to talk a bit about the components of the security risk assurance framework.

>> KEVIN BUTLER: Thanks, Vijay. And let me talk now about, well, first, we will talk about risk assessment methodology, which is based on how we effectively structured the way that we discuss risk in the report. So this is based on the cycle of plan, do, check and act and the monitoring review really depends on the particular stakeholder in the ecosystem. For example, a regulator who reviews a controls or audits that are done by the provider.

So knowing who you are as the stakeholder and these will be context dependent depending on the jurisdiction that you are working in, what role you are playing in the ecosystem. So the context is necessary in order to have that effective risk assessment and evaluation and analysis.

But effectively, this is a, as I mentioned, this is a cycle where you start by understanding the context of what it is you are examining. You monitor and review, you determine what type of risk you are looking at, and whether those risks are acceptable. And then you communicate those risks and you go through this iteratively to really determine what all of your potential risks are.

So those of you who have heard me speak at ITU events before know that usually when I come in, I'm coming, I often come in and bludgeon you with a variety of ways in which your system can fail until you are left in an existential crisis wondering about your life choices so let me play that role again today. The summary of DFS ecosystem threats is really a, this is how we have effectively examines what the threats are against all of the various stakeholders within the DFS ecosystem.

So we have gone through and systemized what these various threats may look like across each individual stakeholder, and the way that we actually ended up structuring the report is that you may notice that some of these threats look common across multiple stakeholders.

So we decided to structure the report first in terms of standardizing the type of threat and then secondly, examining from the perspective of the stakeholder. Now, what we have done that's different in this work is that we have actually as Vijay mentioned, created a list of 117 different controls or mitigations in order to deal with the threats that are based on the vulnerabilities that we discuss. So when you come out of here, you should feel take whole lot better about things. We have a plan.

 Basically the primary stakeholders we look at are the user and we include the mobile device with the user, the mobile network operator who themselves have a variety of network elements in their net York including the base station and telephony infrastructure, the DFS provider who is in charge of communicating with the user, and third party services such as payment providers and other elements of the system.

So now with regard to those third parties, we did examine threats based on the apps and digital wallet framework as well, and I will very briefly talk about that. So from the standpoint of a mobile payment application and device, the threats are similar to what we established on the previous slide. In this ecosystem we have merchants and the types of things they have to worry about include malware on operating systems, compromising of QR codes, man in the middle attacks against point of sale terminals, the ability to relay credentials fraudulently and use those for attacks.

Acquirers are the ones that have to deal with payment system or payment compromise of their network and infrastructure. Payment providers have to ensure that they are not vulnerable to software attacks. As well as design and implement flaws within gateways and systems. And the issuer who deals with issues of payment processing to ensuring the integrity of the system against compromise as well as underlying infrastructure and feet work is appropriate. We consider merchants acquirers payment providers and issuers to be a third party providers and under is other work on the side of the payment service provider that may be best examined in documents like the CROE.

So let me, so going back here, notice that we have identified this wide variety of threats against the system, and I believe we identified 16 different standardized threats, actually 17 different standardized threats. So, for example, 8.17 cover the unauthorized disclosure of personal information, which is of, which is important from standpoint of user, the mobile network operator and the DFS provider. So now what does this actually look like in practice? This is sort of the heart of the report itself, and I want to walk you through one of these threats so that you get a sense of what we are examining in the reports, how it affects the various stakeholders and what some of these controls or mitigations look like.

Let's take a denial of service attacks as an example. What's a denial of service attack. We characterize them for this report as being attacks designed to prevent services within the digital financial services ecosystem from being offered. And we primarily focus in this report on the affected entities being the MNO, mobile network operator and the DFS provider so this is covered in section 8.7 of the report.

So like I said, we start with the notion of a threat. We identify the stakeholders, and then we discuss the risks, the vulnerabilities, and the controls. As we mentioned at the outset, what is a vulnerability? It's the thing that makes your system potentially exploitable. What is a risk. The risk is the means by which you exploit ‑‑ a threat is the means by which you exploit that vulnerability and the risk is what happens if that vulnerability is exploited by a threat. So with denial of service, when we look at things from the standpoint of the mobile network operator, the risk they have from denial of service include the inability to perform transactions due to service outages or transaction failures due to high delays so why is this possible? That's why the vulnerability details. The vulnerability could exist because of network failure due to insufficient network capacity, or due to maintenance or due to design.

Now, in ITU we looked at those eight security dimensions, and the dimension that this targets in X805 is availability. So what are the controls that you can have as a network operator to mitigate this vulnerability and prevent this threat? Control 22 in the Document is as the mobile network operator should take steps to ensure network, high network availability to allow access to DFS services through USSD and SMS and Internet. The MNO should perform technical capacity tests simulating different transactions based on customer numbers, expected growth, expected number of transactions and expected persons with disabilities to ensure continued system performance. You can tell that every implementation is going to be different, but we provide guidance in terms of how you would actually go about dealing with these threats and providing you with the guidance on how to deal with the vulnerability that we have described.

Now, at the DFS provider, the risks are the inability to perform transactions due to a service outage, the failure of a transaction due to high delays or unauthorized access to user data, and the vulnerabilities in this case are three fold, a network failure due to insufficient network capacity, a lack of monitoring of network traffic and individual packets or potentially enabling unnecessary services and these speak to the security dimensions of the availability, communication security and data confidentiality.

Now, what are the types of controls you can put into place in order to try to mitigate these vulnerabilities and threats? So the controls we have identified are the following. The DFS provider should protect against network attacks by using fire walls and traffic filters, protect against DFS infrastructure threats by challenging suspicious traffics. And another control says inbound Internet traffic should be limited and continuously monitored. And set restrictive fire wall rules by default, do white listing on ports, use packet filters, and continuously monitor access to white listed or otherwise permitted ports and IP addresses.

So the report doesn't tell you how to go and configure a fire wall. You should read the Document for your particular firewall to do that, but it does provide you with the best practice guidance in terms of what you should do in order to ensure that you are mitigating risks, and the controls are designed with the DFS ecosystem in mind.

Now, another thing we did in the report is develop a template for application security best practices where we discussed general best practices for a mobile money security framework and this draws upon GSMA study on mobile money best practices, work from ENISA. And so we are going to talk a lot more about this in tomorrow's session if you come to the application security framework session, then you will discuss that, you will also see the, my long held wisdom that every technical presentation in computing has an XKCD cartoon that's associated with it.

If you don't know the story of Bobby Tables come to the session and find out more. The security assurance framework is designed to provide guidance to stakeholders within the DFS ecosystem. The difference between this report and maybe some others is that it's not designed to be static. It's designed to be a living Document. Why is that? It's because the security landscape is constantly changing. Technologies are changing and the mobile environment is constantly changing. Mobile is one of the fastest growing and fastest evolving areas of all of security and of all of computing, I should say actually, and a lot of the most interesting things that are happening are being pioneered on a mobile platform.

So the technologies are changing which means that the vulnerabilities and attack surfaces are changing. The goal for this Security Assurance Framework is to be a living Document where the security advice will evolve as new technologies, vulnerabilities and threats are discovered. I wanted to say in conclusion a great things to Vijay and to Arnold and to others who have provided us with a lot of starting points for putting this comprehensive Document together. Thanks.

(Applause).

>> MODERATOR: Thank you Vijay and Kevin. It was a great summary of the report. I would now like to turn it over to Rehan Masood from the state bank of Pakistan who will review regulatory perspectives.

>> REHAN MASOOD: Thank you Amy. So the key words of today's session I would like to take away is collaboration and partnerships, regulatory frameworks, implementation and assessment of compliance by the providers. So in I would quickly like to share what we have been doing in Pakistan regarding DFS in terms of security, and in term it's of protecting the whole value chain. Because DFS is Pakistan is about extending the inclusion of financial services to the unbanked or underserved segments of the society.

So if we leave the segment open without security regulations you are leaving unsuspecting customers to the threats and vulnerabilities which this report presents. So briefly about DFS landscape in Pakistan, DFS is the cornerstone of SPPs, financial agenda. Pakistan is home to over 160 million biometrically verified SIM connections with more than 73 million of them being the 3G, 4G or connectivity, which is about 45 percent of mobile subscriber base and it remarkably stands at 77%. In contrast, banking services have been concentrated to like 16 percent of the population.

So in order to deliver in 2008 to facilitate synergies between telecom and banks and we were one of the very few regulators in the region come up with the regulation to kick start the mobile financial services or digital financial services market in Pakistan. So today our mobile financial service industry comprises of 12 licensed providers which are offering a variety of ADCs through financial banking services. The synergies between telecos and bank is all for telecos to have some level of ownership in micro finance banks. So we were discussing in the morning to create the synergies and the incentives for the telecos to protect the value chain.

So there because telecos have some kind of ownership in micro finance banks, this is the incentive for putting in mitigation measures is very strong for the telecos as well. So as of first quarter this year, more than 38 million process banking or disability financial services accounts have been opened while over 4,000, 420,000 agents are servicing access points for financial services. This has allowed customers without a bank, without a bank account in far flung remote areas to receive and send in minutes using formal financial challenge and receive welfare payment on question half of Government and non‑government agencies so with the high cell phone penetration, 77% high Internet usage, 45 percent of the mobile subscribers is using Smart Phones because of the cheap data rates and cheap mobile Smart Phones allowing integrations of mobile operators and the majority of the population is under the age of 45, Pakistan has all of the necessary ingredients to set digital revolution for financial services.

So we have recently launched national payment system strategy with the recommendation to design national payment systems complying with international standards and best practice with the help of our colleagues from The World Bank. So this is a brief overview of DFS security environment in Pakistan. As we have been discussing since more there are safe, secure and DFS system possible through collaborative approach through partnerships as there are multistakeholder involved in banks, telecoms and third parties. Realizing this the state bank of Pakistan signed an MoU with telecom operator. Banks are offering digital financial services arriving on the telecom services network. Identification, identification, digital identification is vital to the mobile and telecommunication industry due to their need to identify customers as part of the core business processes, but also because they provide mobile in forms and services to other industries and sectors.

>> So high levels of mobile penetration contribute to open the door to if financial services including payments at the lower cost of financial services allowing mobile service providers to operate an important gateway to expand these services through their authentication processes. So we were discussing in the morning today, we have a very similar organisation, it is called national database and registration authority. NDRA which has registered more than 121 million adult citizens of Pakistan. We have multiple biometrics of these citizens and Pakistan's ID card has evolved into a smart EID. That can meet the challenges of a digitally connected world.

So the Government has also mandated biometric verification for the assurance of mobile Sims for the opening of bank accounts, for the activation of digital financial services. Then on the ‑‑ so we have a major cybersecurity incident last year in one of our commercial banks and since then we have mandated that biometric, the biometric‑based verification is essential for the access of disability financial services apart from the user ID and password. So multifactor authentication is in place for activation of all financial digital services.

Then we have the customer concerned requirements with this additional ID as ‑‑ digital ID, if you want to activate some of your services to consent, to give, obtain your content, the provider has to first verify that you are who you claim to be. So they can do this through this biometric activation, bio metric verification provided by NDRA.

So on the regulations front, I totally agree what Mr. Leon Perlman said in the morning that any regulations has to be principle based or outcome based because if you start regulating a particular technology, you would end up chasing shadows because technologies change overnight, literally overnight. So what we have done in this, in the technologies regulation space is we understand that to do the DFS right, you have to do the ID security right. So we have this technology governance framework in place for banks and micro finance banks and DFS providers which search the security baselines and requirements for the governance and deployment of technology in their enterprise.

And then we have, as I said earlier, we have branchless banking regulation, it sets out minimum requirement for a bank or DFS provider to join hands with the teleco to providing the DFS services, and they set out the risk‑based requirements for different sectors of the customers and now we are working to come up with a mechanism in order to assess compliance by providers to the regulations.

At present we have mandatory regulated vulnerability scans and penetration testing for the DFS systems. However, we have also issued these regulations on mobile banking interoperability by joining hands with the telecom regulators and these regulations set out the criteria for unified interoperable accounts. We have number 9 which set you out the criteria for biometric clarification of all customers who are availing these financial services through apps or through interim banking. Now we are working on an app security framework again to provide the regulatory baselines for the development and deployment of payment apps, Smart Phone based payment apps by the providers.

So in the end, I would like to highlight again that the major challenge is not the issuance of regulations. The major challenge is how to assess the compliance with those regulations. As a regulator, I would like to protect the whole value chain to provide end‑to‑end data security, but how do I ensure that the providers because, you know, there is always a tradeoff. The providers would always like, as someone said in the morning, that security is mostly an afterthought, and we would like to inculcate the security by design, by issuing these, the set of regulations we shared and I shared in the previous slides.

So we are also stud starting to develop an oversight approach to develop compliance with regulations, one of the methodologies discussed is the CROE methodology, and we are starting it to provide oversight expectations to the industry to implement and operationalize the security in the mobile and digital financial services ecosystem. Thank you.

>> MODERATOR: Thank you very much. Now, I do want to turn it over real quick to Dalit Caspi‑Schachner who is remote right now. I want to make sure there are times for questions so make sure we are under ten minutes, Dalit Caspi‑Schachner, if you are on, you have the floor.

>> DALIT CASPI-SCHACHNER: Can you hear me well?

>> MODERATOR: Yes.

>> DALIT CASPI-SCHACHNER: Good. So you can go to the next slide. I will try to share with you what we are doing as our bank, and look at the implementation of many of the things that you discussed today. When I think about managing a risk in general, I think about the basic model of the triangle. The base is the business value, the business objective of a company. As a bank, we are tested of our revenue in the end of each quarter alongside with the expectation to bring value to our stakeholders.

The second side is the risk assessment. The risk assessment of threats, and this is identification of the risk factors and hazards that have potential to cause harm to our organisation. It can be cyber risk and cyber threat, of course. It can be credit risk and it can also be anything that would harm our business goals.

The third side is the risk management controls. This is how we prepare for the threats, for the realization of the threats, and how we lessen the effect of the threats if they are realized. Next, now I will elaborate on each of the sides. When we talk about business value, the public and, of course, our regulator have expectations of the financial system, and justifiably so. We are expected for integrity and confidentiality which is obvious, but also availability meaning we are supposed to be available anywhere and anytime, not accessible to have an ease of use of our application and give our users user experience that is even fun. And they had to minimize the friction between our clients and our digital platforms.

We see an increase in mobile activity and we also encourage it. There is a trend in Israel that many of the bank branches are closing and will give much of our service through mobile platforms, but today not all services are accessible through mobile. For example, large transactions, many people prefer to use the computers and not the mobile.

There are unique characteristics for mobile applications, developers, and challenge for developers and cybersecurity offices. There is a variety of platforms, variety of operating systems, authentication is different than on a PC, and what we are doing and try to rise to the challenge is to build our applications in a bit sized chunks. All of these services you can have in one website of bank of Hapoalim, but when looking on the application, you have an application for each, I would say, not an action, but field of action. So, for example, the open account is a very heavy application because you need all of these kinds of authentication when you open an act, so this is heavy and you probably will just use it once.

We also have a payment application, a stock market application, business application, and account management application. And this way the applications are both light, so it can be supported by different devices and also when we are making changes, the ease of change is helping us so that the testing will not be throughout all of the applications but only one application. This brings us to business value. It's friendly and easy and mostly we try to work through it in a fun way.

Next, please. The second side of the triangle is the risk assessment. So we heard a lot about risk assessment as I understand. We try, we begin with a very good intelligence. We have experience teams and research officers including attack vectors and they build the threat profile for the bank, meaning what are the trends all around the world are relevant to bank Hapoalim in Israel. This way we build situational awareness, meaning we understand organizational vulnerabilities.

Then we combine all of this intelligence and situational awareness with deep knowledge of the bank systems and we build attack vector scenarios. Then we analyze the damage and we find stress scenario. Stress scenario is it a scenario which is high impact. So the damage of the scenario is high, for example, a vast amounts of money are being stolen or there is a major data leak.

Then we decide which scenarios we want to mitigate, and which ones ‑‑ can you return? Which ones we want to mitigate, and which ones we want to accept the risk. You heard a lot about controls today, but not necessarily you need to mitigate every risk. It depends on the risk assessment, and on the risk assessment in which scenario is a stress scenario for you. Not necessarily a stress scenario for bank of Israel, but will be a stress scenario for DFS and anywhere else.

Third is the risk mitigation. The basic SDLC, which means security by design, which is incorporated in the development of the application. This will minimize the risk even in the beginning of the project, and we have an architect, a cybersecurity architect who is accompanying the developers and helping them with methodologies and tools.

Then for the basic ways for controls, if you can choose the stuff for controls. It you push the star.

 Can you go to slide 7. Okay. I will speak and hopefully we will understand without the slides. So what I'm talking about controls, for example, controls that deal with mobile, there is the organisation side, and there is the client side. So organisation side is what I do on the client's device. For example, I can do data separation, and I can disable features. Probably many of you remember that a few weeks ago there was a vulnerability that was published in the Samsung S10 Galaxy, and there was a vulnerability in the fingerprints. So many banks around the world including our bank decided that we are disabling the feature and don't allow our customers to use it.

Returning for the client side, I don't have much control about the client. So I can ask him to make automatic updates, and also sending notifications, but it's up to the client to decide what he wants to do. So what I can do in order to handle this is if you can go to slide 10 somehow, it would be very convenient. If not, I will try without it.

Is to adopt a risk‑based approach, meaning we are looking at ‑‑

>> For whatever reason, it's frozen. It's not moving. I think there is a bug in the presentation.

>> DALIT CASPI-SCHACHNER: Okay. So I will try without it. So the risk‑based approach is looking at from one side of the user and device. We look at the user, and ask for physical qualification, for example, the GPS of the device, we try to understand whether our client is inside Israel or is outside Israel. We use the biometric sensors and we have physical authentication.

Then we look at technology calls risk, meaning which kind of device is this. Is it patched well enough or not? And then we combine both of the user and device and build logical criteria. We look at the behavior of the user inside the device.

So, for example, how he uses the device, the speed that he moves his finger around the screen. We can look at the usage history, did he log into Gmail from this device or not. And we post everything into an AI and try to understand what is the risk of the user and the device. Then we look at the financial action. You want the same way swift transaction that is billions of dollars the same we you treat a transaction that you pay your baby‑sitter.

So we look at the financial risk of the action, the specific action. We can use action limits and we can also use antifraud. The antifraud tests financial behavior of the user, and if something is wrong, like, for example, this client usually transfers money once per month on the first of the month, and now he tries to perform transactions all day throughout the month, then it will raise the antifraud flag.

Then we need to decide when the user and device risk is in alignment to the financial action risk. Then we can decide whether we allow the action or we block the action or we can return to the user and device authentication and try to minimize the risk. In order for it to be in line with the financial action.

So to conclude, we see huge burst of mobile financial activity, and there is a move from cash to digital. Alongside we see, of course, increase in cyber threat, both quantitative and qualitative. So we can ask why bother at all. So, of course, FIGI, it is about this is the main wane for them to get financial services, but for people in Israel, there is a threat potential for this financial system, because people who want to move people from the PC to the mobile, and this is what people would like to have because they want the services to be anywhere any time and easy.

And now our role as cybersecurity specialists is to enable this security activity anytime, anywhere, and with less damage as possible to our both clients and DFS. Thank you.

>> MODERATOR: Thank you.

(Applause).

>> MODERATOR: I know we have a few minutes left here. I will ask one panelist question and then we can open it up to see if there is one or two questions from the floor here. So, Kevin, we heard a lot about the security assurance framework. Can you explain what kind of tools are available for the regulators or others looking to use? Dalit, if you could put yourself on mute.

>> KEVIN BUTLER: The types of tools we have for assessment really vary. There is, depending on where in the ecosystem you are as a stakeholder, from the standpoint of general ITD best practices, if you are running a network for running a DFS provider, then many of those have been well Developed in terms of frameworks for assessment use while on devices, for example, how to actually sort of comprehensively assess a device or an application for its security is still somewhat of a work in progress. The types of assessment tools we have, some of them are automated, a lot of them require manual efforts so putting together a unified assessment framework and tooling system for them is still very much a work in progress.

>> MODERATOR: Thank you. I'll open it up to the floor. Does anyone have any questions they want to ask the panel? End of day. Everyone is tired. Okay.

>> AUDIENCE: My name is Noah from Zambia. Just to the last presenter regarding the mobile security, should brought something interesting about getting, using geolocation in terms ever analyzing data analytics and being able to determine whether the users are within country. I want to get perspective from her regarding citizens consent in relation to them using that kind of feature? Is it something people are happy about because I know we have been having issues back in our country, and maybe if I could just get it from an angle.

>> MODERATOR: Dalit, did you hear the question.

>> DALIT CASPI-SCHACHNER: It depends on the client of the application. He can allow us to use his location, and he can disable the option. So you just need to agree to the terms and this way we can consent a legal problem if this was the question.

>> MODERATOR: Yes. Thank you. Anybody else? We will take last question here.

>> AUDIENCE: I am from broad come, but this time I would like to speak as working party Chairman of Study Group 17 in ITU‑T, I have a strange feeling when I hear all of what I have heard. The feeling is that we seem to have methodology and term and all of that, so why are we failing still today. What is the gap? What is missing between the theory and the practice. So, of course, it will be a long conversation. I'm not going to make it now, but probably I would like to have some further discussion after the fact, but I think there is something that we are not measuring between what we are doing at Focus Group level after ISO level add ITU level and so on versus the cold reality of the state of cybersecurity today. And I would like to invite the people here to think about it, because if we don't look at that in the eyes, it's going to get worse very quickly and especially when 5G will be launched because the attack surface is going to explode and we have no way to tax that activity. Thank you.

>> MODERATOR: Thank you. So food for thought for the panelists for afterward. I would like to thank all of the panelists if we could give them a round of applause.

Thank you for your time and your presentations.

(Applause).

 And I believe we have closing remarks from Bilel. Thank you.

>> BILEL JAMOUSSI: So thank you very much for all of your attention and energy staying here all day until almost, well, past 6:30. We have a nice reward waiting for us, delicious Lebanese food and Tunisian music at the cafeteria as a reception tonight. Before we go there, I will take a few minutes more of your time to quickly summarize some of the key takeaways of the full day. We had the nice session about the SS7 vulnerabilities and the demos that showed the reality of those vulnerabilities. As you know, some of you, the SS7 protocol was Developed and published by the ITU in 1988, which is the signaling protocol for the telephone network and it was discussed this morning, built in a time of trust where the interconnection between operators was physical and it was a closed group. Of course, when we introduced VOIP and mobility, a lot of those assumptions became no longer valid. That was why 30 years later we are now looking at addressing some of those vulnerabilities.

Authentication was also another very interesting session where the password is no longer a viable solution, and we are now looking at new recommendations from ITU, the ask 1277 and 1278 which are based on the FIDO alliance work, which provide a much stronger authentication. And we will have a deep dive on that tomorrow in one of the parallel sessions on the decentralized ID and FIDO.

Then we looked at the DLT security, and Leon and the team have explained the report, and kind of the current state of affairs or state of art with the DLT availability, key management, privacy, et cetera. We also looked at a number of use cases of DLT, Moja loop, and consensus. On the DFS security framework we just had, we talked about risk management, the support on the Security Assurance Framework, the app security template, and tomorrow we will have more of a deep dive in the sessions.

So tomorrow we start at 9:30. And we will not be in this room. We will be in the Mombrion building. We will be heading towards it for the reception. That's where you received your badge this morning. We will be on the first floor of the Mombrion building. We will have five parallel sessions, one looking at how to implement decentralized ID authentication in DFS, full day, tracking of digital Ponzi schemes, also a full‑day session, the implementing app security policy which will be half day, homomorphic application in digital finance will be a two‑hour session in the afternoon and Jamie was Googling what homo morphic means and it will be an interesting session I can assure you. Implementing FIDO implications will also be a full day session.

As you can see on the screen, the photos of the day have been posted on Flickr. You can find them on the ITU web page at the bottom there is the Flickr link, and all of the photos from the session are posted there including the group photo. And we encourage you if you have Twitter to include the hashtag for the ITU financial inclusion.

Today's session is also recorded. You will find a webcast archive on the home page of the program, so we will be able to share the proceedings of today with your colleagues at home who are not able to participate. For tomorrow, we have the parallel sessions. We will try to record all of them because we know that you may not be able to be in multiple rooms at the same time. So, ladies and gentlemen, thank you very much for your attention. I would like to thank very much the moderators and speakers. Both here physically present and remotely.

Also I would like to thank the team that worked on making today's possible, today's session possible, and invite you to the Lebanese dinner, the cocktail reception, and the Tunisia music. Thank you very much.

(Applause).

 (Concluded at 1840).

\*\*\*

This text is being provided in a rough draft format. Communication Access Realtime Translation (CART) is provided in order to facilitate communication accessibility and may not be a totally verbatim record of the proceedings. This text, document, or file is not to be distributed or used in any way that may violate copyright law.

\*\*\*