Harland Clarke EMV Defined Webcast 09/10/2015

TRANSCRIPT

Presenter: Greg Kuyava, Senior Product Manager of Card Services, Harland Clarke

Matt: Good day, and welcome to the webinar. Today's topic is EMV Defined. This webinar is being recorded and will be provided to you along with the presentation recording and deck within a few days. I will now turn the call over to Greg Kuyava, Senior Product Manager of Card Services with Harland Clarke. Mr. Kuyava, you have the call.

Greg: Thank you very much, Matt, and welcome to everyone on this EMV Defined call. This is one part in a three part series of webinars that we are producing around EMV. We've already gone through the full series earlier in this year, and now this is our second time through. We're excited that we still have such a high attendance for this. A couple laundry lists before we get started. First and foremost, I want you to notice on your dashboard, there are a couple of handouts that are available for you to pick up. Some PDFs that give some information around our EMV product and service. We're not promoting that today, but that is available, as well as how our call center and contact center can support you. Look at those handouts. A replay and the PowerPoint of today's webinar will be distributed to all attendees within a week.

Also, if you'd like to ask a question, there are two ways in which you can do so. The first one is you want to use the Panel button and under Questions, you can type your question in to the panelist and the organizers, and we will be able to get those questions. Then, at the end if you want to raise your hand and ask a question via the telephone, that is also available, where you will be able to just click on the Raise Your Hand logo also located in your panel on the side.

With that being said, let's talk a little – let's get into today's presentation. As Matt has said, my name is Greg Kuyava. I am the Senior Product Manager for Card Services. I have been working in developing the different aspects of all of our card programs, including obviously the EMV program which we have been out on the market for the better part of a year promoting our educational implementation and communication strategies around that. I am also an active member of the EMV Migration Forum, and I sit on two of their working committees, education and communication as well as their Instant Issue White Paper Committee.

How are we going to handle today's program or today's webinar? We're going to go into and talk a little bit about what EMV is. This is EMV Defined, so we're going to make sure that everyone has a basis on which their knowledge is for EMV. We're going to look at the trends that are occurring with EMV in the market and how did we get here today? We're going to get in some additional details on EMV and the breakdown of the cards themselves, then get into the project management of EMV and some of steps that need to be taken. Then, we will also handle any Q and As towards the end.

Throughout the presentation, there will be a couple of polls that we will take just to get the insight and some feedback from you, our audience, on where you are in your EMV migration. At the very end of this presentation, we just ask you to hang on for a quick exit survey to share with us how you felt about today's content, and other products and services, or other pieces of information that we can be providing you.

Let's dive into this, and let's go into our first slide in the EMV overview and talk about what is EMV? EMV comes from the payment networks that originally developed the specifications. The E, and the M, and the V, stand for Europay, MasterCard, and Visa. Now, really what we're talking about when we are talking about EMV is an interoperable standard that specifies and governs the transaction between the chip card itself and the terminal at the merchant. Now, global interoperable standards have been around ever since there have been credit and debit cards. This is just the next phase in the evolution of security around the secured card industry. If you think back at the different steps when it comes to globally interoperable standards first, there was the embossed lettering, the size, and the type of fonts that was allowed as well as the indent print on the back. The addition of the magnetic stripe is a globally interoperable standard. You look at the hologram as well as the logos that were added. Each of those came along at different phases and were enhancements to the card in order to – I should say with enhancement to security of the card, and EMV is just looked at as the next step in the evolution of that security. What it does is it allows us to create a stable basis for investments in chip-based payments across multiple form factors.

Most cards that are being introduced to the market right now are a contact card, meaning the chip comes in contact with the reader. There is also contact chips as well as contact list devices. Think about things like key fobs or that are attached to accounts and of course mobile devices, your mobile phone being able to be utilized in this type of environment. EMV makes sure that as we have innovation in these different products, there is still a very stable ecosystem in the interoperability of that payment transaction doesn't get compromised.

What is EMV really going to do? The next slide really talks about that. First and foremost, it is going to be reduction in the fraud. In all the markets where we've seen EMV introduced, fraud on the debit and the credit cards have reduced significantly. With the occurrence of data breaches there is a risk and an operational cost that are associated with card programs. With fraud being reduced your operational costs are going to be able to come down.

Now, the initial investment in EMV obviously going to be greater than what you paid for a magnetic stripe, but in the long run you're going to reap the benefits of a reduced operational cost because of the reduction in the amount of data breaches. It's also going to help you in the risk management. Any time fraud is reduced your risk management becomes better.

The other security around this is how the cardholder and their verification features are going to be handled. Now, until merchants become 100% EMV-ready, it will still support traditional magnetic stripe type of transactions. All EMV cards that go out there will have both an EMV chip as well as the magnetic stripe. The issue themselves – you on the phone will actually be able to define multiple cardholder verification methods that you can define, and you can determine whatever the conditions are at the merchant, they can hit a hierarchy of how you want that card – not only the card to be verified but then the actual holder to verify that they're the right person. Then, it also allows for a security around offline PIN as well. Those types of transactions. Transactions that do not occur in real time can still be an EMV transaction in an offline environment.

Moving along. The impact of EMV also changes things significantly. When we look back at the magnetic stripe, and we think about what it would take to set up the magnetic stripe program, there were a set of keys that were shared between card partners, your EFT processor, and your card personalization or your card issuer partner. Those set of keys, and the information tracked, data tracked, placement kind of determined how that program was going – how that order was going to be processed, and then it was going to work when the transaction needed to be processed as well. In those circumstances you did not need to coordinate a setup with both your EFT processor and your card personalization provider. Both of those partners could work independently to set up the program because they're utilizing the same set of keys. When it came time to test your program and test cards, you knew that the functionality was going to be there.

Also, part of a magnetic stripe environment or magnetic stripe program, your card manufacturer did not need to coordinate or know what the specifications or the requirements were from your card personalization vendor or your EFT

processor. They could go ahead and produce a standard debit and/or credit card, any kind of secured card, knowing that it's got to have a magnetic stripe, it's got to have the hologram, and you have to know what association it was, the placement of all those elements on the secured signature panel, those types of thing. We're all very standard, and they've been around for quite some time.

EMV actually changes all that. EMV requires a coordination of the project that insists upon your personalization provider, your EFT processor, and your card manufacturer all working together sharing the information so that you can make sure that the element that you're putting on the card coincide, and are certified, and work in the environment at your issuer as well as in your EFT processor.

Not only is this happening on the issuing side, but it's also happening on the merchant side. They're also having to make sure, with their merchant acquires, that the software they put in place will be able to work properly and will be able to run the EMV transaction as needed. The impact of EMV really affects all the parties involved and has become a much more integrated approach as far as coordinating all of your partners at once.

Let's talk a little bit about the market and EMV and information that is available. In 2011—we'll just keep forwarding through these slides, Matt, if you wouldn't mind. In 2011, both Visa and MasterCard came out with their liability shift announcements. Up until that point, it was really a discussion within the industry itself, the card associations, the EFT processors, the personalization vendors, the manufacturers, all of those, about this migration that's going to happen with EMV.

Then, the holiday season of 2013 hit, and the data breach that occurred at Target became front page headline news. All the cable news networks continued to have it as their lead story, and it continued because of the timing of it and because of the retailer that got hit for a matter of weeks. That's truly the conversation went from, "What happened?" to "How many accounts were affected?" to "What can financial institutions do? What can an individual do? What can the industry do to help protect this data and help protect the card program?"

At that point, EMV started becoming part of the vernacular, part of the discussion for the cardholder, as well. The spring of 2014 hit, and it seemed as though we were dealing with or hearing about a new data breach every single week, if not every single month. As you can tell from this slide right here, there were a number of large retailers that were being hit and were affected by the

data breaches which then, again, only emphasized the number of cardholders that were being affected.

In 2014 alone, there were over 700 breaches that were publicly disclosed. We only heard about the really big ones. Of those really big ones, you can count the ones right here just on this page on basically your two hands. Seven hundred breaches in a year, which was a significant increase of almost 25% over the year before that, really shows that the merchants are being affected by this, even though it might not always be front line news.

I mentioned the liability shift, and we're going to talk about this real briefly in the next slide. As I mentioned, Visa, MasterCard, as well as the other associations came out and they said, “You know what? We're going to have this liability shift.” The reason behind this is that it's important that the United States being the only market in the world that had not started to migrate to EMV yet. We need to make sure we migrate over to that. Data breaches were occurring at a more significant rate. The number of cardholders that were being affected was increasing substantially year over year. The idea to launch the EMV was an industry-wide initiative.

Visa/MasterCard didn't regulate or mandate. There weren't any laws passed in Congress, but what they said is, “Come 2015, we're going to set dates up for first, the EFT processors to get their stuff in place. Then the merchants, we want them to be ready by 2015. We know that the banks will then follow along. The issues will then follow along at that point because the merchants will be asking about it.” What we're really doing here is we're just on the precipice of this liability shift and what's happening.

The liability shift itself—what does it mean and what are the differences? Let's go to the next slide and we'll talk about liability shift in a little bit greater detail. Essentially what's going to happen is in a transaction, you're going to have an issuing card or a cardholder that is going to have an EMV card, and you're going to have a merchant that's going to have an EMV point-of-sale machine. A transaction that occurs in environment number one where the EMV card is presented but the point-of-sale at the merchant is not able to accept it as an EMV transaction. It'll still be able to be run as a magnetic stripe transaction. However, the liability for that particular transaction will fall now on the merchant itself. That is the shift in liability that occurs. EMV card presented; non-EMV transaction that occurred because the merchant was not up and running with their EMV system yet.

Then in an environment or a transaction that a merchant has their EMV system up and running but the card being presented does not have an EMV chip on it,

that transaction, again, will be run as a magnetic stripe transaction. However, the liability will stick and stay with the issuer just as it is in today's magnetic stripe world.

In the last scenario, you have an EMV card being presented at a merchant that has an EMV terminal that is fully ready. That transaction is run as an EMV transaction. Once again, that liability will stay with the financial institution. However, because it is an EMV card run at an EMV terminal and it's an EMV transaction, the fraud and the opportunity for fraud is reduced significantly.

Really what the liability shift does is it puts an incentive out there for merchants to get their point-of-sale machines up and running. For all those transactions that do not happen or that get run through their systems that are not EMV-ready, the liability goes onto them.

What we're seeing is we're going to see that come the liability shift, the larger retailers are going to be more prepared and ready than the smaller ones, rather it's more resources, more money to be able to invest in this type of thing, we're seeing statistics anywhere from 50-60% of retailers in general are going to be ready come the liability shift. Over 40% of the market is—the merchants are still migrating their systems over. Obviously, because the larger retailers are the ones that're more prepared, that means the smaller vendors are much slower to adapt to this new type of security.

The other interesting statistic that we're seeing—if you click just one more button here—is that we are actually seeing—there was a prediction that we're going to see a rise in criminal activity between now and when merchants are going to be fully ready to handle EMV transactions or to 100% versus the 60% we're going to see come the end of 2015. Before the window fully clothes, experts are predicting a rise in criminal activity and actually, we are seeing that is coming true. Over the last couple of months, we are seeing an increase in the number of data breaches that're occurring.

Really, what it comes down to is October 2015, the world is not going to end if your EMV card is not in the market. Many of you are working on it. Obviously, many of you are educating yourself on what you need to be doing. However, you want to get that program up and running as soon as possible just to reduce the fraud and then reduce your liability around those transactions.

That brings us to our first poll question of the webinar. We will post up on the site here so you can answer, but we're asking when will you have EMV cards distributed to your cardholders? A, currently in the market or you will have cards by the October liability shift; the next four to six months, which kind of puts you through Q1 or Q2 of 2016; you're beyond Q2 of 2016, when we talk

about seven months or longer; or you know what? Just haven't decided if you're going to do it yet. We're seeing less and less people answer this question this way, but there certainly are a number of them out there still trying to figure out what their plan is. I'm going to sit quiet here while we give you a chance to answer this question.

Great, looks like we had almost 70 of you on the phone today; 70% of you answered the question. What the results are showing us here is it looks as though the big majority, 58%, are between the four- to six- month period. That doesn't surprise me at all, that being the largest one. Certainly anecdotally, our customers, the ones that we are talking to, are either just starting or are in the process coordinating getting the project started.

Those that were a little bit more proactive, we're seeing them fall in 31%. Those are the ones that probably reached out to their EFT processor towards the beginning of 2015 and got on their queue. We were hearing way back in March, April, and May that start dates for people that were trying to get their EMV program up back then weren't even until August, September, October of this year. Many of you fall into the next two categories, the four to six and the seven months, mostly because you just – the queue is too long. There's a bottleneck of so many financial institutions coming into it.

We still have a couple that're undecided which, again, doesn't necessarily surprise me because this is complicated stuff, and you need to know how it affects your financial institution, and you need to know what resources to put into it. You need to educate yourself on what are we doing and why are we doing this? I appreciate that.

Let's see. Any questions up to this point? It does not look like we have any questions as of yet, so we're going to continue on. Let's now transition into the structure of the EMV card and get that down in the more nitty-gritty details of what that looks like. The EMV card itself, as I had mentioned earlier, will have both a chip and the magnetic stripe on the actual card itself. That will not change as far as having the magnetic stripe and magnetic stripe transactions being able to occur.

Now, the magnetic stripe itself will be embedded with information that details and indicates that this is an EMV card. If it is presented at an EMV-ready terminal and is swiped, the terminal will read the information on the magnetic stripe and will not allow the transaction to go through until it's presented as an EMV transaction. In most cases or in all cases that I've seen so far with my own EMV card, there are instructions on the terminal that you need to insert the card into the terminal and present it for the transaction.

What we have as far as construction goes is you still have your front and the back of the card just like you would – like it normally would happen. In a chip-only card construction, what happens is the chip actually gets embedded into the card itself. There's really two parts of this chip that you're looking at. You have the face plate, which is the big, gold plate that you're looking at. Then underneath that is the actual chip itself that actually runs all the transactions and handles it and acts as a mini computer. Chip-only construction means that you're only embedding a chip into it.

Another type of construction would be a dual face or dual interface type of construction where you still have the chip and you have the face plate, but running within the card itself is an antenna. In a dual interface card construction, it allows for both a contact transaction—card presented to terminal and contacted with the terminal, or a contactless transaction where it is using that antenna as an RFID type of transaction. Then it's running the transaction without it having to come in contact.

Within the card itself, you have card platforms or the operating systems. You basically have three to choose from; Native, Java, and MULTOS. We'll get into those, definitions of those in a little bit. You need certification within the card itself. Again, certification needs to come from the card associations. Then the chip itself, really the minicomputer that is on here, holds not only the cardholder data but it holds special encryption keys as well as the certifications for that particular EMV card so we know it can function correctly.

Let's take a deeper dive into the different card types that are available. Now the size of the chip itself will come in two different sizes. You'll have an eight contact or a six contact. Now for a contact card, again a card that is only presented and needs to come in contact with the terminal itself, there really is no difference between the eight contact and the six contact. You can certainly choose either one. The eight contact, because it has eight contact points on it, takes up more real estate, so it's a larger chip, which leaves less real estate for the financial institution's brand. The eight contact chip is also a little bit more expensive than the six contact chip. As far as functionality goes, as far as it being able to handle the transactions, the six contact size chip is just as good as the eight contact chip.

We were talking about contact, and again, these are the first two. These cards are what is inserted into the reader. What is different than the magnetic stripe function is that in all EMV transactions, that card stays in contact with the reader throughout the full transaction. Only once the transaction is over and has been approved will the card be ejected.

In a dual interface, again, you still have – you're going to go to an eight contact chip with this because you'll need the larger chip for the antenna that's running in the inlay of the card, but it can function both as a contact card as well as a contactless. Again, by utilizing the antenna, which uses RFID to communicate with the terminal that a transaction is occurring.

The chip itself is comparable to a computer, which we'll talk about here in the next slide coming up. Think about the chip, the little contact plate in the chip that resides on the contact plate, is the hardware. It's very similar to the shell of your laptop, whether it be a ThinkPad or be a Dell or an Apple, some sort of PC from Hewlett-Packard, those types of things. The chip itself is just a piece of hardware. Just where there are multiple or many options that there are when it comes to computers, the type of hardware that you can purchase, there are literally hundreds of different chips available out there. In the case of an EMV program, your card manufacturer will be able to steer you in the right – in the chip manufacturers or the chips that they have available.

In a computer, what resides on that particular hardware is an operating system. Again, it might be DOS, might be Windows; could be Mountain Lion. This really helps in the actual hardware to operate and to handle any other applications that you put on top of it. The chip in EMV is no different, and there are three operating systems that are available: Native, which is a proprietary operating system, Java and MULTOS, which are more globally utilized operating systems, and I'll get into those definitions in the next slide. However, on top of your operating systems are different applications. Just like you would use your Excel, your Word document, Lotus Notes on your laptop or your PC, you have different applications that go onto the operating system for the chip.

However, when it comes to the applications for an EMV chip, it's going to be very specific to the card association; Visa, MasterCard, American Express, Discover, all have their very specific applications. If you have a Visa card, you're using the Visa 1.5. If you have MasterCard, you're using the M Chip. You have very specific applications based on the card association you're with. There's a comparison between how a computer operates to what the EMV card is. It really is just putting a small microcomputer onto your card.

Let's talk a little bit about the operating systems and what are available out there. Native, when we're talking about Native, we're talking about an operating system that is a unique personalization script. It is developed specifically by either the ETF processor or the personalization provider and for that particular financial institution. Often times, it can be less expensive but because of the uniqueness in it, switching or going to a different type of operating system would require all new development. Switching from one personalization

provider to a second one or a different processor from an existing one requires your EMV program to all be set up again.

Multiple applications are possible within this. There's an advantage; we talked about the applications on the last slide. You could have multiple applications on the same card at the same time. Because if you're creating this script uniquely, production lead time is a consideration.

The other two platforms, Java and MULTOS, are both open platforms. Really what this does is this creates more interoperability with systems that are out there. The time to market becomes much quicker because they're not creating unique script for this. They are more open for personalization set-ups, and the more EFT processors as well as personalization providers are going to be operating on either a Java or MULTOS. It's just making sure that you coordinate with your EFT processor and your personalization provider, that the personalization provider is encoding the same operating system that your EFT processor needs.

Between the two of them, Java is a more robust operating system, thus it might be a little bit more costly. However, besides just handling financial transactions, it gives the capabilities or the abilities to add additional features and functions to that chip. If you're thinking forward, it would provide the opportunity if you wanted to use this for transit or ID, security, whatever the case might be. Java, as far as the United States is concerned, is about 80% of what is being introduced into this particular market as an operating system. It's a financial type of transaction operating system. There's no security enhancement of either of these two open systems or the Native. All three of them provide the exact same amount of security. It's just that they're the type of functionality that you want on the chip itself.

Alright, let's dive down into the next application and AID and get into those in a little bit more detail. Now we talked about the operating systems, and you're going to choose one of those three that goes on the chip. Now the applications themselves and the AIDs, application identifiers, are the next things that need to be layered onto the actual card itself or the chip itself. The payment networks and the terminal specifications define the requirements for the software on the card and how the terminal itself will employ the EMV toolkit.

The application will be determined based on the card association that your card is associated with. If it's Visa, you're going to use a VIS application. If it's MasterCard, you're going to use their application. Then the merchant will be – just as you see a sticker when you walk in the door, “We accept these cards,”

the merchant programs their EMV readers to handle all those different cards and the applications of those different card associations.

The AID, the application identifier, is a data label that helps differentiate between the different payment systems and different payment products. At this point, the issuer uses the AID to identify what applications are on the card just – and the merchants help identify which is on the terminal. What happens is at the merchant, the terminal itself, the point-of-sale terminal itself, will also have application identifiers. The cards and the terminals will talk to each other and see which AIDs are mutually supported. Once they see which applications are mutually supported, they will then initiate the transaction. Both cards and terminals will support multiple AIDs.

From a credit card perspective, again, it'll mainly be dictated by the card association. However, in the debit world, because of the Durbin Amendment and the debit cards needing to support multiple networks or allowing merchants to choose from multiple networks in order to route the transaction, there need to be put in place an alternative AID apart from the Visa AID or the MasterCard AID. Many of the networks got together and now have what is called a US-common AID.

When that card is presented at the terminal, what's happening is it's recognizing that this card's a Visa card, so it has the Visa AID as well as the US-common AID. Then the terminal looks at it and says okay, we support Visa as well as we support the US-common AID. Then the merchant determine which rails they want to have that transaction go across. Both the cards and terminals will support the AIDs. They will have multiple AIDs on those cards.

Alright, let's transition now into the security around this now that we've set up – we have all these different elements that go on the card but really, what are they doing? We keep talking about the EMV payments are going to be more secure and the transactions are going to be more difficult to duplicate; fraud is going to be much more difficult to initiate. How is that all going to work? We've got all these features, got all these things that are going on there. So far, it's really just costing us more money to put a chip on there, and an operating system on there, and AID on there, and all these different types of things.

What happens with the security of an EMV transaction is really sets the security into three ways. First is the card authorization, and this is a method that is determined to making sure that the card is not counterfeit. EMV is a card-present security measure. Any time EMV is on a card, it is protecting that card against any type of recreation or creation of a counterfeit card; thus, in a card-present transaction, that transaction cannot happen. Card authorization,

making sure that the card is real and it's not fraudulent is the first step. The way that happens is it communicates with the terminal itself, and then it verifies that based on the information on the chip itself, it's a good and active card, and it's not fraudulent.

Then we go into the cardholder verification method. This is the person that's presenting the card to the merchant, are they the rightful card holders? Again, the financial institution will have a number of cardholder verification methods they can choose from. Really, what we're doing, again, is protecting against a card that is lost or that is stolen and that the rightful owners is the individual presenting it.

What an issuer will be able to choose from is they'll be able to choose do they want them to just be able to sign for the transaction like they are today? Do they want to require the individual to enter in a PIN? If they're entering in the PIN, does that terminal need to be online, or could it be in an offline environment? If it's under a particular dollar amount, do we not require our cardholder verification method at all? A lot of the methods that are available today in a magnetic stripe world are still available here. Because of the encryption that's involved, the cardholder verification method is an added level of security.

Now the merchant or the financial institution will decide of these four, maybe all of these four, what is the hierarchy in which they want to have cardholder verification method? If the merchant themselves – they'll decide which CBMs they will actually support. They will take a look at your hierarchy and which CBMs you have on your card and then they'll, again, match it up with which ones they're supporting. Then the transaction will go based on what are the first two matching hits. The issuers, as I just mentioned, you prioritize your list of methods for chip verification.

Last but not least is then the transaction authorization, and the authorization controls, and the encryption codes that come back with the card. Not only is the transaction going through and what's happening is we are going through this full encryption as well as this whole set of verification methods and verification calculations that are occurring. Then they're creating numeric sequences that are tagging this particular transaction and bringing it back. At the end of the day, if the numbers don't match up, if the numbers don't work, then the transaction doesn't allow it to go through. What's happening here is that it is allowing for the authorization, and this is really where EMV comes in and does its work is that it's authorizing that particular transaction.

Now in an offline scenario, the card – offline, again, I'll just define that quickly. Offline is where the merchant itself is not handling this transaction in real time. The telecommunication portal is down. What happens is if your financial institution allows for a transaction to go through in an offline environment, the card will then act on behalf of the issuer to either allow for approve or not approve the actual transaction at the point-of-sale.

Let's take a break here. Let's go to our second poll question of the day. It talks about what we just talked about as far as the different cardholder verification methods. Now there – we have 58% of your folks that were getting ready to – actually we were closer to 80% within the next six months putting the cards out there. Please share with us what is your FI's preferred cardholder verification method? We'll have you choose from either signature only, online PIN, or offline PIN.

Alright, it looks like we had about 60% of you vote on this one. Pretty even, right down the middle, we have signature only. That doesn't necessarily surprise me because when we look at migrating to EMV, what a lot of financial institutions are trying to do is keep the experience as similar as they can to magnetic stripe transactions. The idea behind allowing the individual to sign for the transaction versus having them do a PIN – they're just trying to keep that comfort level with the card.

Online PIN, again, this doesn't surprise me where it comes in right around 50%. We're seeing an increase in this because it's the added security. A signature can certainly be copied. However, a PIN is something that's personal and is something only known to the cardholder. It just adds an extra level of security.

Offline PIN, 7%. It's those individuals that are looking to provide a little bit more convenience when it comes to transactions. When EMV first came out, I would say Visa was strongly encouraging signature-only types of transactions, and they weren't encouraging PIN transactions. MasterCard was encouraging both signature as well as PIN transactions. I wouldn't necessarily say that either one of those card associations have tempered their views on that. Oftentimes, signature and online PIN break down whether you're going to be Visa or whether you're going to be MasterCard?

Alright, let's talk a little bit about this EMV project. You know what? Before we do that, it looks as though we did have a question come in, and so I'm going to pause here and take this question since it does talk about swiping the card. The question is most consumers are used to swiping. How do you recommend informing consumers to use EMV instead of swiping? Excellent question, and it really ties into the comments that I was just making. What we're trying to do in

this EMV migration is to use the – is to make sure that the change in the card itself isn't a true disruptor. By that, I mean it discourages the user from using their card. That's a loss of opportunity. That's a loss of revenue.

Couple of things; one, you need to be able to educate your cardholders prior to the cards being distributed. We'll talk a little bit about that communication strategy at the end of this, and I would also highly encourage you to participate in our upcoming webinar that talks specifically about educating and communicating out to your cardholders. You need to be able to communicate and educate them on how the transaction is going to be different and let them know that the card will be coming in contact with the point-of-sale and it's going to sit there until the full transaction.

Secondly, the card itself, on the magnetic stripe, if it is an EMV card and the terminal is EMV ready and it needs to be run as an EMV transaction, it will not allow that card to be read as a magnetic stripe. The terminal will read it, will read the magnetic stripe, will see that it's an EMV card, and it will then indicate to the individual that they must insert the card as an EMV transaction.

Target, within the last couple of weeks, just launched their debit card EMV. I went to the terminal and as I was using my card, I saw the instructions were to either swipe or insert card into the reader. Now I certainly knew what they meant by insert the card because I'm living and breathing EMV every day of my life. However, I wanted to see what the terminal would do if I were to run it as a magnetic stripe transaction.

Sure enough, I swiped the card. It actually sounded an alarm and then it instructed me on the terminal itself to insert the card into the EMV reader. Then as the card was in contact with the reader, it said, “Please keep the card in the reader for the full transaction.” Then when the transaction was done, the alarm sounded again and it said, “Please remove card from the reader.” The card itself, the reader, and the EMV terminals or the point-of-sale terminals will be able to communicate with one another and then provide the instructions to the cardholder. Education's a big part of it.

Someone said yep, Target has all new terminals, too. Target just got its debit card program up and running.

Alright, let's talk a little bit about the EMV Card Migration project. As I mentioned earlier, this isn't your grandfather's card program anymore, right? It is completely different. It takes a lot of coordination. It takes a lot of learning and education along the road. It can be extremely overwhelming if you don't understand all the different steps and everything that goes along to it, whether it's training yourself on what EMV is and what we need to expect, to defining

what your program's going to be, to coordinating the personalization of the EFT processing side of it – wow, we've got to redesign our cards, so now marketing should get involved, and we have to make sure that our manufacturer is producing the chip with the right operating systems on it so it can actually be encoded correctly at the personalization provider. Wait a second, there's more keys I have to handle. There's just a whole bunch of things.

What you really need to be able to do is you need to be able to get yourself with a partner that can simplify the whole journey, and this next slide shows a little bit about what Harland Clarke does for program management. Matt, if we could just forward quickly. There we go.

What we want to do is – whether it's Harland Clarke who has a fully complete, Chip Complete, if named, program management, or someone else, you want to be able to partner with someone that can simplify this whole process, one through seven steps, migrate you through this in an orderly fashion. We also need to remember that you're managing some key partners.

Let's forward onto the next step, as well, and how do you have to manage those key partners. You've got your card manufacturer, your card issuer, and your card EFT processor. As I had mentioned at the top of this webinar, in a magnetic stripe world, all three of those could act pretty much independently. There were a set of keys that were associated with the card program along with a VIN number that allowed the card issuer as well as the EFT processor to set up your card program on both of their systems independently. Then by the time it came to test the card, you knew everything was going to operate correctly because they keys that were shared between the two companies were matching.

The card manufacturer, as the third partner on this, could be completely independent. They just need to make sure they had the right magnetic stripe, they had the right card association, they had the right logo, the right signature panel, and they created the design the way you wanted to. With EMV, the type of chip that's being used, the type of operating system, the applications that need to go on there, the AIDs that need to be run, all of that takes coordination between the different providers. Not only that, but providers need to be certified with one another in order to prove that this card personalization provider can work and has worked with and has been certified with this EFT processor. There's just a much greater need for coordination between all of your partners. Managing those key partners is extremely important. The next slide is just an overview of how these different elements actually overlap with one another and again, how you're going to need to be able to manage those.

Next slide, real quickly, we're talking a little bit about when to migrate to EMV. Now most of you are already migrating to EMV, so I'm not going to spend a whole heck of a lot of time on this other than to say that you want to move through this process as quickly as possible. As the experts have predicted, their predictions are coming true. As the window closes on this type of card fraud, the fraudsters are going to increase their activity. Those financial institutions that continue to wait to get their EMV program up and running, their transactions will become the most susceptible to data breaches. They will then be increasing their risk as well as increasing the amount of fraud.

Alright, last but not least, this last section that we're going to talk about is simply the cardholder communication strategies around this. I will again plug look for an upcoming webinar from Harland Clarke that goes into greater detail on consumer education and communication. Why is it so important? First and foremost, we want to continue to create that positive customer experience. Things are changing for them. The way the transaction is going to be handled is changing for them. They're going to be at a terminal, and they're going to try and run a magnetic stripe transaction, and they're going to get bells and whistles pointed their way in order for them to do it.

You need to be able to help them through this process to make it less stressful. The card being held in the terminal for the full time is going to be different from when they swiped with the magnetic stripe. Maybe they had to hand it over to the attendee at the cash register, but oftentimes they're able to put it right back into their wallet. You want to be able to make sure the experience through the whole process is a positive one.

Also, you want to make sure that as EMV now is becoming part of the discussion for the cardholder, you want to make sure that your financial institution is fully committed to their security of their account, and you want to make sure that they recognize that you're doing everything within your power to safeguard their transactions and their data.

As you educate and as you communicate out, you're going to increase your card activation and usage. People will be more likely to use a more secured product but more importantly, you're going to significantly reduce your attrition. You are reissuing new cards. As you reissue new cards, it's going to require an individual to call up and activate that new card. You want to make sure that they are comfortable and they understand the importance of activating this new card because it's going to provide them more security, and it's going to protect their data. It's going to protect them from the data breaches like Target, and Home Depot, and Michael's, and some of the other restaurants and retailers. They need to understand that, and that will drive them to actually activate that card.

Equally important is you want to make sure that you are minimizing the impact to institutions' internal resources. As these cards go out into the market, again, you're going to see an uptick in questions coming back to your financial institution. The more you've educated yourself, the more time you've taken to educate the consumer on the front end, the less questions there are going to be. What is your strategy, then, to handle those additional increases in phone calls? Are you going to utilize a call center? Are you going to have something on your website that educates them? How are you going to educate your internal employees on how to handle those types of questions? These are all things you're going to need to be able to consider and put in place as you get ready to introduce this.

Last but not least is just a sample of the recommended best practices. When we're talking about communicating, there's really three stages in which you want to communicate. You want to communicate prior to the card actually being issued. It's going to be important that you do that. We recommend 60 to 90 days prior to that. Obviously, some financial institutions on the phone don't have the 60 or 90 day luxury in order to be able to produce that communication. Any communication prior to the card being issued is significant and important and will be helpful.

I belong to a very large financial institution. They sent me a letter indicating I'm going to be getting a card in the mail. I was thinking it was going to be another two or three months. The card showed up a week later. It was good for them to inform me it was on its way, and it listed some stuff and what they wanted to do.

As the card is being issued, the cardholder – you want to be able to, again, provide instructions to that individual as to what this card is, why is it different, the benefits of the security that you're adding to it, and then what they need to do in order to activate the card. Then the ongoing and continual education – people are going to go out there, and they're going to be able to use the card at some merchants as an EMV transaction. They're not going to use it as an EMV transaction at other merchants. They're going to have questions. They're not going to understand why the point-of-sale is screaming and making bells and whistles at them. They're going to have questions. Think about what your ongoing education strategy is going to be, whether it be call center, follow-up emails, electronic, whatever the case may be, but it's going to be important.

Alright, that reaches us to the end of our webinar this morning. Again, I just want to thank everyone for the – for your time. It looks as though there are no additional questions that've come in. There are no additional questions that have come in. I'm just going to, again, let you know that we do have a couple

more webinars on EMV that are coming up. One of them is on our EMV chip complete program, which is a more in-depth look at what Harland Clarke can provide from and EMV standpoint, as well as a communication education webinar that is coming up that really gets into the strategies and the messaging behind education and communicating your cardholders.

With that, I'm going to thank everyone. We do have an exit survey, so if you would just hang on, we'll launch that survey. We would appreciate your feedback you have for us on this webinar and the information on how that – and the information that we provided. Thank you, and have a great day.