Harland Clarke State of EMV: Countdown to 2014 Webcast 07/08/2014
TRANSCRIPT

Presenter: Nicole Machado, Director, Card Services

Presenter: Greg Kuyava, Senior Product Manager, Card Services

Ann: Good day everyone and welcome to the Harland Clarke State of EMV Countdown to 2015 conference call. Today's conference is being recording. At this time, I would like to turn the conference over to Nicole Machado. Please go ahead.

Nicole: Thanks Ann and welcome everyone to today's webcast, the State of EMV countdown to 2015. My name is Nicole Machado and I'm the director of card services here at Harland Clarke and my colleague, Greg Kuyava, who is the senior product manager for card services at Harland Clarke, will be taking you through this webinar today.

I just have a couple of quick housekeeping items to discuss here at the very beginning. We will have two ways to submit questions to us. Certainly we want to get through as many as we possibly can. The first would be to submit your question through the chat function on the webcast and you'd want to ask your question to all panelists and then we will get to as many of those as we can at the end. Second, if you would prefer to ask it in person, you can certainly at the end of the presentation, we will open it up for questions and Ann will be able to tell us how we go about doing that. As well, at the end of the webcast, we will make a PDF of this presentation available for all of you and a follow-up email with a link to the webcast will be sent out in about a week to all attendees so you can look for that as well.

Lets go to the agenda. A couple of things we are going to go over today, we're going to give a quick EMV overview, where we are in the market today, what's happening with EMV, then we're going to go into our survey results, the bulk of this presentation, and what insights are leaning from that. Finally, we're going to go through some slides on how to prepare for EMV. What you're going to need to know, what kind of questions you need to ask, who you need to ask them to, how you prepare your financial institution and then lastly how can Harland Clarke as a partner help you in your EMV journey.

With that, I'm going to pass it over to Greg and he'll take us through why we should even be considering EMV.

Greg: Thank you and I'd like to thank everyone as well for joining us this morning. For the next three or four slides, we're going to level set as to what is going on in the EMV market today as Nicole had said. The first slide will handle why financial institutions are migrating over to EMV. You'll see some of these main reasons also play out in the survey results that we're going to show you in just a little bit. First and foremost is I think financial institutions are looking at a way to increase the security on the actual cards

themselves whether it be credit or debit cards. The consumer is certainly becoming much more educated in regards to what an EMV chip is and what that chip means as far as security.

As we look to increase and improve the security of the cards, what we're also doing is fighting the migration of fraud into the United States. It is well known that the EMV card has been used in markets all over the world outside of the United States for the past 20 years. What naturally occurs is the United States is becoming the main target as the fraudsters start looking for markets in which they can easily have an advantage in gathering the data on these cards. We are seeing that more and more of this type of card fraud migrating into the United States. In order to stop that migration, EMV is the next step. . The EMV chip can also help in minimizing the risk associated with the card program within the financial institution.

There's also a global interoperability that is being requested by card users as your cardholder travels to an international destination. Being able to use their card whether it be at a restaurant, retail kiosks or transportation kiosks is important.

Last but not least, it's also an innovation in the payments industry. It really is the next evolution in both debit and credit cards, not only in security, but also what and how these cards are being used. If we look at European markets and the Asian markets in particular, you're seeing that EMV cards is a big part of the transportation network. The evolution of using these cards for multipurposes for not only debit or credit transactions and access to the account, also then for other purposes like be public transportation, a student card or government issued id. You're seeing financial institutions looking to migrate to an EMV card based on providing the most innovative payment structure to their cardholders.

The next slide deals with the key dates in EMV migration. This is the past, present and future of what's going on. This is to make sure everyone has the most current and recent information on this. Back in 2011 is when Visa and MasterCard announced their plans for EMV (in what everyone is referring to as a liability shift in the United States at the point of transaction). In 2013, the processors started supporting the EMV transactions or at least that was their deadline in order to be able to support EMV transactions. What we're seeing now is the merchant acquiring processors and the POS systems that are going in at the merchants, are begging to meet the EMV compliance date. Every day reports show how more and more merchants are able to handle EMV transactions. If you know what you're looking for when you go out to your local gas station or your local pharmacy or your local large retailer, you'll notice that many of them already have the POS equipment in their stores. It's just a matter of getting that equipment up and running on the appropriate EMV software and platforms.

2015 is the big date that everyone looks to and talks about when it comes to EMV. That is usually referred to as the EMV liability shift. This is not a mandate and this is not a new regulation that's coming down. It is a date or a time frame from the EMV co. (Visa, MasterCard, American Express), that they have put together for the United States trying to provide an incentive to merchants to be EMV ready. If an EMV card is being presented as a merchant and that merchant is not able to handle that transaction as an EMV transaction, the liability then shifts onto that merchant itself.

© Harland Clarke 2014

What is happening now with merchant processors and the POS systems getting set within retailers, directly reletes to the ability of that retailer to receive that card, recognize that card as an EMV card and then handle the transaction in the appropriate manner. As long as the merchants are in compliance with the new EMV "rules", the liability then stays at the financial institution. Those merchants that do not have the EMV ready equipment and cannot handle an EMV transaction after 2015, you will see a shift in the liability for that transaction.

The future of EMV will next go to the ATM machines and their ability to handle their transactions on accounts via an EMV card. Finally in 2017 the automated fuel dispensers, the AFDs, (deemed as more difficulty in preparing those machines) will be EMV ready.

Another note worthy event that has occurred, other than the announcement back in 2011 by Visa and MasterCard on their plans for EMV, was in 2013. Everyone is familiar with the Target breach that occurred right around the holidays. There was also Michael's and Marshall's department stores that had a breach on the card information stored within their systems. That became the top news items for a good two and a half week period. This event and the way the news covered it brought the consumer into the EMV discussion. Up until that Target breach, the deadlines that we've highlighted on this page have been more of a discussion between the card associations, (Visa and MasterCard and AMEX), the card processors as well as the financial institutions and their partners (the card issuing partners and their card manufacturing partners). EMV to the everyday consumer cardholder was not something that was top of mind or something they were very educated about or even knew about. The Target breach changed all that. As the story went from "here's what happened" to "how can we protect ourselves in the future," EMV became a very big part of that discussion. Because of this new consumer awareness, more financial institutions are focused on bringing this type of EMV program and security to their cardholders.

The last slide that I'm going to cover today (before we get into the survey results) is about EMV cards in the global and US markets. You can see the way we have this broken up into the different markets outside the United States with the two European zones, the Asian pacific zone, Latin America, including Canada as well as the Caribbean, and last but not least, the Middle East and African markets. Those have been the markets that have supported EMV for the last 20 years so obviously the card percentages and ratios are going to be much greater. The penetration rates and adoption rates are going to be much higher. When you add up all the other markets outside of the United States, you're going to see that there's over 2.3 billion EMV cards in usage right now. This is a report that comes out on an annual basis and it shows that EMV usage continues to increase throughout the world.

In the United States, as we would anticipate, our numbers are much smaller, only hitting 20 million in total. Most of that is due obviously because we're just now adopting the actual EMV program, financial institutions are getting their programs up and running as acceptability in the merchants is becoming more available. As we get closer to 2015, you're going to see the 20 million EMV card number continue to increase as well as the adoption rate in the number of EMV terminals available. WE anticipate that both of these numbers are going to increase significantly over the next 18 months until we hit that liability shift date. The only other note that I would make on this; as far as the United States estimates,

that some people would actually say that 20 million estimate is fairly low based on what manufacturers have been distributing out to their banks. . Whether it be 20 million or 40 million or 60 million, the EMV card is certainly coming to the United States. There are incentives in place for both the merchants and the financial institutions to have this program in place. The consumer is aware and getting educated on it. The consumer is requesting it and is asking it for purposes other than travelling over to international destinations. They're wanting it for security. When it comes to migrating fraud, when it comes to mitigating the risks, it makes sense for a financial institution as well.

Next, we're going to transition into the survey results. To level set for everyone on the phone; in 2013, Harland Clarke submitted a survey out to its financial institution partners and we did a similar webinar on those results. What we will examine are the results and a comparison between the 2013 and 2014 EMV surveys. . With that, I'm going to transition back to Nicole and Nicole will take us through the first couple of slides of the survey.

Nicole: Thanks. The initial survey results. We surveyed over 750 financial institutions ranging in size and ranging in card based, so the respondents ranged from $50 million to more than $1 billion in assets and from 2500 to more than 100,000 annual card volume. This survey really went across the smallest of financial institutions to some of the larger, so we got a good cross section of respondents.

Our first question was we wanted to level set. We wanted to find out has your financial institution started researching EMV. In the past year, financial institutions have made some significant progress in their research of EMV and beginning to lay the groundwork for implementation. As you can see here in 2014, over 90% of the financial institutions surveyed had begun researching EMV compared to just 74% of last year. That's good news for all of us that everyone is getting more and more educated on EMV.

The next slide is a positive slide from our standpoint. As you can see, compared to last year, financial institutions have begun to engage and start discussions with their partners who will be with them on this EMV journey. A year ago, only 47% of the respondents had consulted their processors while here in 2014 that number has risen to over 73%. I will say the one number on here that is a little concerning is that only 35% of the respondents indicated that they consulted with their card associations be it MasterCard, Visa, American Express, Discover etc. The reason why this is concerning is we are hearing that it is taking several months for card associations to open up projects for financial institutions on EMV because the number of financial institutions in their queues continue to grow. The card association is going to be a critical component in these discussions, but we can also see that financial institutions have reached out to their issuers, their manufacturers at a greater rate this year than last year, so it's great to see that financial institutions are engaging all the partners that are going to be required. Everyone listed here be it the processor, the associations, the card issuer, the card manufacturer and of course the financial institution themselves are all going to need to be engaged in working together to move these EMV programs along.

Here is the good news. Respondents are feeling more confident about their knowledge of EMV now than they were a year ago. In 2014, 75% of the respondents feel somewhat knowledgeable or very knowledge about EMV compared to only 53% last year. The percentage of financial institutions that

don't know where to begin or don't know where to start have dropped from 17% in 2013 to just 6% in 2014. That is good news that everyone is becoming more knowledge and are educating themselves on EMV. I'll turn the next few slides over to Greg.

Greg: Thank you. I think it's that increase in knowledge about what is going on with EMV and how to implement an EMV program that also shows us a shift as we look at time frames for implementation. You can see as we get closer to the 2015 liability shift, naturally it's going to shorten the time in which financial institutions will typically implement their EMV program, so you see a natural increase in all the categories from 0 to 6 months, 6 to 12 months, and 12 to 18 months. What also is happening is all of these time frames (even when you get out to the far reaches of 18 months), all of them fall within being ready for the 2015 liability shift. What's probably more important here is that as financial institutions are becoming more knowledge about implementing an EMV program, part of that comfort level developing their strategy and their time frame in order to implement that program.

That then leads us into our next question as to how or to whom do you plan on rolling out your program. Again, what we look upon here is there is a significant decrease in "upon request" going from just a little closer to 30% to all the way below 20%. I think when we also then compare that to when "we reissue our cards" and also as a "mass issue" strategy, both of those strategies are increasing. Financial Insitutions are understanding how they want to roll out their EMV cards, Equally important is that they are taking a very proactive approach. They're no longer waiting for someone to come in and ask them for an EMV card The advantages and differences between the two; mass issue helps you get the cards out immediately, the FI can predict all of the costs and you can handle them all at once. When you reissue cards upon their expiration dates, obviously it does it on an extended time frame, but it still allows the financial institution to control he cost while issuing in a time frame suitable to their card holder needs.

The next slide that I'm going to handle is the main reasons for migrating to EMV. As you're looking at this chart, the colored chart wheel itself is the response percentages back from the 2014 survey. The main reason for migrating to EMV, 44% in the 2014 survey said "fraud deterrent". You'll notice in the parentheses right next to fraud deterrent, the 38% represents the 2013 results. What this particular slide is showing us is that from 2013 to 2014, the results haven't varied greatly. It's still liability shifts and fraud deterrent making up over 78% of the reasons why people want to migrating EMV. As we talked about in the opening of this webinar, when we talked about reasons to migrate to EMV, fraud deterrent, handling liability migration, risk, all of those are shown here in this particular question. Nicole, if you'll lead us through to the next slide.

Nicole: Great. What type of EMV program are you considering? This slide is a little interesting because we saw earlier that about 75% of the respondents felt very knowledgeable or somewhat knowledge about EMV. However, this slide suggests that while financial institutions may feel knowledge about EMV in general, they may not be as comfortable with their specific EMV program plans. As you see here, more than half are still undecided about the type of program their institution is going to roll out. Of those that have decided, it is split almost evenly between financial institutions that are going to roll out an EMV chip only program or a dual interface, which is chip and RFID. I just want to make a quick

mention here that either way a financial institution chooses to go whether it's EMV chip only or using dual interface, all cards in the United States as least for the foreseeable future will always have a magnetic stripe.

When we talk about dual interface, that does not mean EMV chip and magnetic stripe; what that means is the EMV chip and the RFID antenna, very similar to money pass of the Visa product where you can tap and go. The reason why institutions are considering dual interface is that sort of the natural step into future forward looking payments such as mobile, etc. We can see that folks are going both ways on that.

These next two questions were new to this year's survey. We really wanted to determine if the widely publicized Target breach had any impact on financial institution's urgency or priority around migrating to EMV. Interestingly, the majority of respondents indicated that the breach in itself really did not change their priority to migrate to EMV, although we do see that a little over a third did indicate that the breach did make the migration to EMV a bit more important or maybe higher in their list of priorities at the financial institution. As I was thinking about this particular question, I would have thought that the Target breach would have had a larger impact, but I think we can deduct from this slide that folks were really planning their EMV strategies long before the Target breach happened.

The next question is how the Target breach increased your cardholder's awareness of EMV cards. Certainly, as we would expect, the breach did heighten the awareness of consumers around EMV as the Target breach pretty much commanded the headlines in the newspapers and on any news shows for a number of weeks over the holidays. While they were talking about the breach, it almost always had a mention of EMV as a way that the US payment landscape could become more secure. I'm sure as financial institutions you all likely noticed an increase in questions from your account holders around this topic, "do you have EMV cards, will I be able to get one," etc.

Finally, when we ask financial institutions about their biggest concerns to migrate to EMV, both the cost of implementation and the cost of issuance were at the top of the list this year just as it did in 2013. We all know and understand that EMV as a significant undertaking from a cost perspective and I think that is concerning. Financial institutions will need to really start looking at their risk portfolios and what's happening in their financial institutions around fraud, what are the losses, etc. when they're looking and trying to evaluate how they're going to roll out EMV, are they going to do a mass issue, are they going to do it in stages, etc. In 2014, merchant acceptance and their readiness as well as a need for consumer education also topped the concerns. I think everyone is starting to realize we're in this together and in order for EMV to have the greatest impact, both financial institutions and merchants are going to need to be on board all implementing the technology to ensure that we are doing our best to mitigate fraud at all points.

What does all this mean? Greg is going to take us through some additional considerations in this section, EMV and the financial institution.

Greg: Thanks. Hopefully by discussing some of the survey results, as your financial institution, goes through and starts creating the strategy, creating a timing, this gives you insight into what your peers

are doing. As Nicole said, what's next? What do we need to do as a financial institution? What are the "getting going" points?

First and foremost, we want to talk about what you need to know about EMV cards. This really starts with education and understand within the financial institution in what is needed. There are a couple of highlights on this slide that the FI is going to need to research and get some additional information on. At one point in time, there was a wait and see period, many FI's not knowing what was going to happen with the Durbin Amendment, and the requirement of allowing debit cards to be to supported by multiple debit networks. The question was whether the card associations were going to change the liability shift date, were they going to change or make an exception on debit cards on this requirement when it came to EMV. There is no change in the liability shift dates and it's still going to go forward. The major card associations and the networks have created a solution that allows EMV to move forward and support the Durbin Amendment regulations. They have created a solution so the FI will still be required to have multiple networks available, enabled to allow for merchant routing choices. It will be important for the FI to make sure the understand what your are you routing and network choices are how you need to be able to set up your EMV program the routing decisions on the actual cards themselves.

You also want to make sure that it is operating and interfacing with the terminals, the POS terminals, in the way that you want it to. As Nicole had mentioned earlier, there's multiple choices for the card to be contactless card, whether it be a contact card or whether it be dual interface. . The FI will make the decision and choose the type of security on the card. The hierarchy in which that card interacts with that POS terminal and in which EMV security measure you require to occur, will determine how the transaction will occur. Knowing all the options, identifying and educating yourself on what the various options will mean to the security of the transaction is going to be important and the basis on your EMV program.

Last but not least, financial institutions need to be able to verify that the all networks that they're working with have signed licensing agreements with the primary card associations. The card not only needs to be support by two debit card networks, but the secondary debit card network will to need to run off of a MasterCard or Visa network (AID). All secondary networks will need a licensing agreement in place with the primary or unique network (AID).

Moving next onto what is needed to get started. Number one is determining the type of card that you want. Is it going to be a contact card, contact chip only, is it going to be a contact list chip with a RFID antenna within the card itself, or are you going to utilize both of those functions and have a dual interface card? It should be noted that cards for the foreseeable future there's certainly no end date or site being talked about. We'll also have the capabilities of running the transaction through a magnetic stripe as well. But what's going to happen is as you present an EMV card to a merchant and you're to swipe it and use the magnetic stripe, but it has an EMV chip on that card, the POS terminal will then be able to instruct the cardholder that they need to run that as an EMV transaction.

Secondly is the FI will need to determine the cardholder verification method (CVM). Whether you want to be able to allow the card to be verified online only or allow the transaction to be verified offline using

a PIN. This all determines how that card transaction will be verified In talking with your card processor and your card associations, you'll be able to determine which is the best CVM for your financial institution as well as what type of card that you want.

Third is setting up the unique application identifiers (AID) whether it be Visa or MasterCard or American Express as your main one, and then your alternate networks, (ie. Star or Shazam). The FI will also have to determine if additional AID applications are needed. Is the card going to be used for transit or as part of campus access like a student card or part of a state ID program? . Those are all additional applications that can go on the EMV card. Once again it comes down to understanding what your needs are and what the card is going to be used for by your cardholders. All of this will help identify not only the main applications in routing of the transaction, but also any additional applications that you want on it.

The types and number of applications on the card will be used for will will also determine the amount of memory needed. Memory needed is going to then determine the chip size to allow for the additional card features,

Once you start understanding what your action item lists are, you now need to start really preparing your financial institution for EMV. That starts with taking a look at what the consumer cardholder's needs are. Is it travel versus domestic usage?

You also want to discuss internally what are the fraud trends in the market and risk to FI in the market. Knowing the risk and the liabilities will determine how urgent you want to set up the EMV market. Are you going to be more of a follower and sit back, wait and see? Are you going to try and be a trendsetter and get the EMV card into your card holder hands now? Are you going to match the efforts of the FI's who have already put over 20 million cards in the US market already? Are you going to wait in hopes to get a better understanding of EMV or maybe by waiting costs might come down. No matter what direction you take, it's all about understanding what your needs are to both control the fraud and the risk to the FI, but also the cost.

You need to engage your card partners and this can't be stressed enough. The survey shows that financial institutions are currently doing a much better job in 2014 than they were in 2013. Engaging your card partners includes the card associations, that includes your card processor, that includes your card issuer and your manufacturing partners. All of these card partners are going to be extremely important to make sure the platforms and the programming that's being created within your unique EMV program is being coordinated by all parties.

Last but not least, you need to set in place your strategy on educating your employees. They need to describe the security and the benefits and the reasons why you're migrating to an EMV program versus keeping the existing card program in place. Also keep in mind the education of the card holder. That could occur in a series of communications via email or direct mail or through statement mailers. Both of these education considerations will allow the FI to prepare in the right way so you're not only ready from an operational standpoint (the card works properly), but then also from handling the consumer as well.

© Harland Clarke 2014

The last slide I'll let Nicole talked about in how Harland Clarke can help you with EMV.

Nicole: Thanks. How can Harland Clarke help? We want to stress to our financial institutions that we can be the one stop provider for both manufacturing and personalization, both at a service bureau perspective and/or an instant issue perspective. We can certainly knock two buckets off of your partners that you need to engage because we can do both manufacturing and the personalization. We can handle both Visa and MasterCard and American Express and Discover. We just want to stress we are committed to being part of your team. We'll have an implementation manager who's going to help collaborate with the rest of the financial institution partners that you have be it your processors, your card associations, networks etc. We're committed to being part of that team and to helping your EMV strategy move forward and we will help to manage your conversion process. We just want to be clear that we're ready and positioned to help you when you are ready at the financial institution.

That's it for our presentation today. We do certainly have some questions in chat and we also want to open the line for questions and I'll let Ann give instructions on how to do that in just a minute. If you have other questions that come up, you can certainly reach out to either Greg or myself; our information is on the screen and we would be happy to direct you to be able to get you the information that you will need. Ann, if you can let folks know how they can start asking questions and then I think Greg is going to manage our chat questions as well and we'll get as many questions answered as we can.

Ann: Certainly. If you would like to ask a question, please press *1 on your telephone keypad. If you are using a speakerphone, please make sure your mute function is turned off to allow your signal to reach our equipment.

Greg: Thank you. Lets give the individuals that want to queue up via the telephone a chance to actually do that. I will start with the questions that came into us during the presentation via the chatroom and answer some of those.

Question: "As an issuer of EMV cards, how will we know if the merchant location where a fraudulent transaction took place has EMV equipment?"

That's a very good question. What's happening during an EMV transaction, as is you're actually programming that EMV card to be identified at the POS as an EMV card. If that transaction goes through and the merchant itself is not EMV ready, Visa, MasterCard, the main card associations will identify that card is an EMV card and then will identify that the merchant was not able to handle that card via an EMV transaction. That's when the liability will shift onto the merchant versus the financial institution. If you were to have an EMV card and you were to go to a merchant that is EMV ready and has an EMV terminal at their POS and you were to use the magnetic stripe, as I stated earlier in the presentation, that POS terminal will then direct the cardholder to run the transaction via the EMV service within the terminal itself, and that typically means slipping the card with the EMV slot or if it's RFID a contact list, waving it over the appropriate area of the POS. The card itself will be programmed to tell the POS terminal how the transaction should be conducted.

Question: "will the magnetic stripe continue to be used actively after the deadline?"

Nicole: The reason why in the United States we are going to have the magnetic stripe on cards for the foreseeable future is if you can think about all the different merchants that we would need to have convert over to EMV technology, all the mom and pop shops, all the cab drivers etc., it is going to be quite a process. The question is "will the magnetic stripe be actively used?" It will really depend on the preparedness and the readiness of the merchants and the financial institutions. Clearly, if the merchant have not updated their terminals, a magnetic stripe will be used for that transaction, but has Greg had indicated, if the card is an EMV card and the merchant as an EMV enabled terminal, the transaction will be run as an EMV transaction.

Greg: **Question:** "What about card not present transactions, how will the liability shift and migration to EMV effect those where the card is not present?"

Nicole: That is a great question. EMV technology at this point in time is not part of a card not present transaction. Those transactions would still be run as they are today using the three-digit security code on the backs of either Visa or MasterCard or the four digit static code on the front of American Express. At this point in time, the EMV technology is really for card present transactions when a card actually is submitted for payment. The liability would run the same rules as it does today for those types of transactions if they were fraudulent activity.

Greg: **Question:** "Is there a date by which financial institutions assume liability if our cards are not EMV?"

It's an interesting question because I think there's a lot of confusion around the dates on the liability shift. At present time, the financial institution is responsible for the liability on a transaction at a merchant. Really what the liability shift is, it's an incentive and a deadline for merchants to be able to handle the EMV transaction. What Visa and MasterCard and the other major card associations have done is they put in place a road map on first lets get the transaction processors to be able to handle EMV transactions. Once we get all of them up and running, lets now go to the merchants and make sure that they can actually at the POS start the transaction process via an EMV transaction in the way that the bank wants it to be able to be handled. Once they have those two components in place, that's where you hear all about the liability shift, that's the merchant processors, that's the merchants being able to handle EMV transactions at 2015. The idea behind this is that once everything is in place, financial institutions will naturally adapt to EMV cards and promoting EMV cards out into the market. The big incentive being for the financial institution is to help mitigate the fraud and help reduce the risk with their card programs because it is a more secured card and it's a more secured transaction. In an EMV transaction where both the merchant and the financial institution are EMV compliant, the liability would still be assumed by the financial institution. It's only after 2015 if the merchant is not EMV ready will the fraud shift to them.

Another question here, "is there a date by which financial institutions assume liability if our cards are not EMV?"

Again, answering back to what we just said, you're still assuming the liability moving forward, it just doesn't shift over to the merchant.

Question: "How does EMV assist with reducing losses resulting from online purchases?"

As Nicole had answered earlier, EMV at this point in time handles card present only transaction, not card not present, which online purchases would fall into.

Question: "Do you have more materials on the different types of EMV?"

There are a number of different types of material available. There's a number of different types of platforms and operating systems in which the card itself needs to be set up, the best place to start is go to your card association and start engaging your EFT processor. They will be the ones that will help you identify which are the different types of EMV cards and operating systems and platforms that you need that will best suit your needs. What I would also highly recommend is creating; an EMV project management team, as well as, having someone or multiple people within your financial institution join up with the different card groups for education on EMV. The EMV migration forum is a great source of resources and understanding what your needs are and understanding the trends are going to be and keeping yourself updated.

Question: "Who can we contact for EMV at Harland Clarke?"

Certainly feel free to reach out to either Nicole or myself and we will be able to then, if we feel appropriate, get you in touch with the account executive or start the discussions internally with you.

I'm going to pause here now and turn it over to Ann to see if there is anyone that has queued up now.

Ann: As a reminder, it's *1 if you would like to ask a question. We'll take our first question from Dwayne Ferrera from State Employees Credit Union of New Mexico.

Dwayne: My question is surrounding the instant issue card machines that we purchased about a year ago. Is there going to be some kind of conversion kit or program that would allow us to still be able to use our Card@Once machines after we start issuing EMV cards?

Nicole: All machines that we had sent out starting October 1st of 2013 with EMV capable. There is programming that needs to be done obviously at the production facility but all the equipment that was sent out after October 1st, 2013 can read and write chips. If your equipment was purchase and received prior to that, we do have some conversion plans that we can put into place to help migrate your equipment to be EMV capable. I have your name here and we will get in touch with you after the call to determine specifically through your financial institution what we need to do.

Ann: At this time, we have no further questions in the phone queue.

Greg: We'll go back to the phone in just another minute or two to see if anyone else has queued up. I'll just let everyone know that if we end up with more questions that we're able to answer within this webinar session, we will make sure all questions get answered in an email and we'll send that email out to all attendees as a follow up to this webinar. If we don't get to all the questions, we'll certainly make sure we send the responses out to those questions going forward.

Question: "Once we have EMV cards, will it be impossible for thieves to make bogus cards like they did after the target breach?"

The technology behind EMV creates what I'll call a dynamic transaction. It is a transaction that continues to have a time stamp to it and the three-digit security code, the dynamic CVV that is created to that particular transaction, continues to change from one transaction to the next transaction to the next transaction. It's almost like creating a brand new transaction with new information on an EMV card versus a magnetic stripe card, which has static information for each additional transaction. An EMV card has programming that allows the transaction and the information for that transaction to change from each one.

Question: "Are cardholders able to select to override EMV in a merchant that has EMV?" Nicole, would you like to speak to that one?

Nicole: I'm not 100% certain what the question is. Cardholders are not going to be in the driver's seat in an EMV world. The financial institution will be making determinations of how they want their cards to be routed. If a financial institution has an EMV that's going to have a different service code on the back, which is going to identify instead of a 101 or 102, it will have a different service code that will identify that as an EMV card. If it's swiped at a terminal and it's EMV, it's going to recognize it and the based on what the financial institution has set up as far as rules, as far as how the transactions can be run, that's what's going to designate the next steps. For an EMV card, it's always then going to indicate if the terminal is EMV capable to please insert your card and run it as an EMV transaction. The issuer is in the driver's seat.

Greg: And since we can capture all the questions in the chat room and email those out to individuals, I'm going to go back to Ann one more time to see if there is anyone else that has queued up in the phone line.

Ann: We'll take a question from Gary Austin from Credit Union of America.

Gary: I was wondering how many financial institutions are going with chip and signature versus chip and PIN, and what are the big financial institutions like Bank of America and Chase doing.

Nicole: Visa is really encouraging folks here to do online transactions so that would be chip and signature. Chip and PIN is really designed to be able to handle offline transactions. In the United States, most transactions are run in an online environment, the lion's share of them. It's really where you start running into some issues with having a chip and signature would be for travellers who are in Paris and are trying to ride the subways over there are at an unmanned automated payment machine that is offline; that requires chip and PIN. The easiest way here in the United States, the most streamlined way to set up a program, is chip and signature because we'll almost a solely online environment but it really depends if you have a huge portion of your based set as travellers and spend a lot of time overseas, you may want to look at perhaps going to chip and PIN as opposed to chip and signature. I do have a card from one of the very large issuers and it is chip and signature. Just because you choose one way to start

and get your feet in the EMV world and to get your programs up and moving doesn't mean you can't at a later date transition to a chip and PIN environment.

Gary: Can a card be used for both types of transactions like chip and signature in the United States and then default to a chip and PIN when it's in an offline mode?

Nicole: Yes, it can be set up that way. That would certainly be one of the parameters that you can choose. There are some considerations that you need to have in place particularly around if your institution offers the ability to choose their own PIN on cards and how that PIN number gets translated back to the cards. There are some considerations and your processors can help walk you through those in greater details, but yes, you certainly can. Any kind of chip and PIN can also be chip and signature. That would be part of your determination as far as what your priority is going to be for a transaction to be routed.

Greg: In other words, you'll determine the hierarchy; is it chip and signature first, if that's not available and if the merchant is offline, do you want to allow for chip and PIN as the next option and finally signature.

Ann, is there any additional questions via the phone line?

Ann: Not at this time.

Greg: We have gone past the end of the hour. I would once again thank everyone for their participation. We will send out a recording of this webinar as well as a PDF of this webinar over the next couple of days. We will capture those questions that came into us via the chat that we did not have a chance to answer and we'll respond to those and send those out via email as well. Nicole, any final parting words of wisdom?

Nicole: No, we're all in this together. We're here to help if we can and you should see on your screen now you have the ability to download this presentation as a PDF if you'd like and we will be sending out those webcasts here in the next week or so.