Harland Clarke Webcast
The Informed Banker TRANSCRIPT

Presenter: Christine Ahlgren, Payments Marketing, Harland Clarke
Presenter: Steve Kenneally, Vice President, ABA Center for Payments & Cybersecurity Policy, American Bankers Association

Jeb: Good day, and welcome to the Harland Clarke Speaker Series, The Informed Banker. Today's topic is EMV in the USA: Chip Matters More Than Anything Else. This audio-cast is being recorded, and you will be sent a link for playback next week. If you have questions, please use the Chat box located in the webinar control panel. Your questions are private and are only seen by our presenters. I'd now like to turn the call over to our host, Christine Ahlgren, of Harland Clarke Payment Solutions. Christine, you have the call.

Christine: Thank you, Jeb, and thanks to all of you on the phone for taking the time out of your busy schedules to be with us today for our first segment of The Informed Banker audio series. We are very excited to bring this community bank focused content to our Harland Clarke clients. On the second Thursday of July, August, and September, you can look forward to learning more about topics relevant to your businesses from a team of American Banking Association experts. After today's call, you'll receive an email with a two-minute survey soliciting your feedback on today's program and also looking for suggestions for future topics. Are you interested in learning more about navigating social media in a highly regulated industry, or how to succeed as a community bank lender in a rising interest environment? We'll gather your feedback, and announce the topic for our July 14 session very soon.

Now, without further ado, I'd like to introduce today's esteemed speaker, Steve Kenneally, who will bring you up to speed with the latest on EMV migration. Steve Kenneally works in the Center for Payments & Cybersecurity at ABA on issues related to a range of payment systems including the check, ACH, card, wires, as well as coins and paper money. He's spending an increasing amount of time focused on emerging payment technologies like mobile payments, virtual currencies, and P2P payments with an eye toward making them faster, safer, and frictionless in the future. He's also a staff liaison to two standing member committees focused on payment issues in addition to ABA's Emerging Payments Advisory Group. Steve served as the Chair to the International Banking Federation Value Transfer Network Working Group, and prior to joining the ABA in 2005, he served at the United States Department of the Treasury where he managed the private network of banks collecting non-tax payments on behalf of the federal government and also drafted regulations and guidance on cash management issues. Steve earned an MBA from The George Washington University and as a fellow Boston College alum, like myself, where he earned a BS in Finance. He is also an Accredited ACH Professional.

Thank you so much, Steve, for being here today. We are thrilled to have you.

Steve: Oh, I'm glad to be here, Christine.

Christine: Wonderful. Jeb, if you wouldn't mind at this time, if you could show the polling question? We'd like to get a feel for where all of you stand in your own journeys toward the implementation of EMV. If you'll take a few moments and tell us how far along is your bank in implementing EMV? You can use the radio buttons on the screen in front of you for those that have that ahead, and then we'll take the results in just a few moments. Great, thank you. Wow. It looks like a good number of you still have some work ahead, so let's get into it. Steve, can you tell us what EMV is, and why are we using it?

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

Steve: Okay. Let's start off with some basics. EMV is a technical standard developed by Europay, MasterCard, and Visa, and it refers to a standard debit or credit card that has a chip or integrated circuit embedded into it. What the chip does is it creates a dynamic authorization when it's dipped at a point-of-sale terminal. That basically means that the data that's associated with that card and that transaction can't be used if it's stolen or breached to create another counterfeit card because it simply won't work. What the EMV card does is it makes your basic debit or credit card, when you're using it using the chip, much safer than your old card that just has the data on the magnetic stripe.

Christine: Thank you. That was a great overview, Steve. I'm wondering. Why is the U.S. moving toward EMV to being with?

Steve: Okay. It all comes down to security, security, security and especially since the U.S. is one of the last places on earth to make the transition. What that has caused is it's made all of the data associated with our magstripe cards a big target for hackers. Everyone on the line I'm sure can recite all the big breaches, whether it's Target, or Heartland, or T.J. Maxx. They could probably also relate to how many times they've gotten the breach notices in the mail, and they've had their own cards replaced. With that in mind, using EMV technology in chip cards is going to eliminate or 99% eliminate counterfeit card fraud using stolen data. What that's going to do is prevent or make that data that's being held at merchants or payment processors less attractive to hackers because they're not going to be able to use it. It's a multi-prong approach where it's going to make the data that merchants are holding less attractive, and it's going to help out banks because they're not going to have to reissue as many cards, and it's going to help consumers who aren't going to have to go through the hassle of replacing their cards all the time.

Christine: That sounds good to me. We all know that there was a deadline, Steve, last October. What was the impact of that?

Steve: Okay. First off, there was a deadline to when it would be a shift in liability between the parties, meaning the merchants and the banks. There was no real deadline, and there is no mandate for the change. It's up to each party to decide whether they want to upgrade their equipment. Basically, what the card networks announced back in 2011 is that they were going to introduce EMV technology, and whichever party, whether it's the card issuer or the merchant, had the oldest technology, the group with the oldest technology would assume the liability for counterfeit fraud. That was the incentive to try to get card issuers to get more chip cards in people's hands, and to get merchants to put more updated devices at their checkout lines.

If a consumer is using a chip-enabled card at a merchant that doesn't process chip transactions and that card is counterfeit, the merchant would assume the liability. If you flip it around where the consumer is using a card that only has a magstripe on it and that card is counterfeit and it's used at a merchant that can process EMV transactions, then the liability shifts on over to the issuer. Just as an aside, since this is going to be a long migration where not all the merchants are going to be live and able to process EMV transactions right away, cards are going to have a magstripe and a chip on them as a hybrid card for years to come until every merchant or a critical mass of merchants is able to process these sorts of transactions.

Christine: That's great, Steve, and you saw from the poll at the beginning of this call that we have a number of bankers on the call today whose banks haven't yet migrated. What does that mean to them?

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

Steve: I mean, if you haven't looked at the economics of shifting, it's definitely time that you start looking at the economics to see if the numbers make sense. If you have not changed, you are assuming extra risk by absorbing counterfeit card transactions if your cards are counterfeited and used at a merchant that can take EMV transactions. You've got to offset that by figuring out how much it's going to cost you to switch. That includes the basic stuff like how much the cardstock is going to cost you. Then you have to add in the more general or soft costs like training for employees and customers as well as stuff like postage.

There's one more thing that I think is important is that I think consumers are finally getting it. That these chip cards are more secure, and you don't want to have a card that people think may be less secure than others that are in their wallet. There's also a marketing aspect where you don't want to fall behind the competition too, too far and be the only one with a magstripe card.

Christine: That makes a lot of sense to me, Steve. You talked about the fact that there's an evolution here of adoption. Can you just talk us through some different scenarios where maybe a merchant hasn't upgraded but the issuer has, or what does that look like in these different scenarios?

Steve: Sure. If the card issuer has upgraded but the merchant has not and a transaction happens with a counterfeit card, then the merchant assumes the liability. It's the other way around if the card has been counterfeited and the merchant is capable of taking the EMV card but it's used – a counterfeit card using the magstripe is used, then the bank is liable. Basically, it's whoever has the oldest technology is going to absorb the liability for counterfeit card fraud losses.

Christine: Okay. You talked about this balance between the risk you're taking by not converting and the cost to convert. Do you see banks or anyone moving towards this change at a slower pace? Does it have to happen all at once, or can you begin migration with new cards for instance? How does that work?

Steve: Yeah. We've seen banks take all different approaches, and I don't think I've seen one that's switched them all at the same time. That'd be a pretty big drain on your resources to switch out all your cards at once. Some banks are taking it month by month and trying to get it all done over the course of a year. Some are switching out their magstripe cards for chip cards during the natural process when cards are expiring. That's a pretty simple way to do it, but if your last magstripe card doesn't expire until 2020, that may be a little slow, depending on the bank, but again, it's up to each bank and merchant to decide when they're going to upgrade.

Some banks, especially the early adopters, focused on their heavy card users and especially their heavy card users that traveled a lot internationally. Because like I said, the U.S. was the last to – basically, the last country to move over, and it was getting more and more difficult to use a magstripe-only card in Europe and Asia and South America.

Christine: Great. Steve, we talked about this being a resource heavy change. Do you have any sense for the true cost of this to issuers?

Steve: I think the costs are going to range a lot. With most things, for smaller community banks, their per unit cost is going to be a lot more than if you had a million cards in your portfolio. Unfortunately, that's just the law of big numbers. You should be able to get an idea of what your card costs are by working through your card processor or whoever is helping you issue your cards and would provide you with the replacement stock, and that's a hard number that you'd be able to assign a cost to. Then you'll just have to work around trying to figure out what your labor and training costs are going to be and if there's going to be a bump in your call

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

center. All things like that when you introduce a new product.

Christine: Okay. Thank you. Do you have a feel for the status from the market overall in terms of implementation for both the card and the merchant? What's their readiness like at this point?

Steve: It's a little bit all over the map, and there are a lot of different authorities out there for at least some studies and surveys and poll numbers. Let me just step in and say Visa announced some numbers just this week. They announced that chip card transaction volume was $20.7 billion in April, and that's up 12½% from March. That's a really big per month jump, so I think we're seeing a lot more chip-enabled cards being released. Visa has $282 million chip-enabled cards out there. A hundred and forty-six million of them are debit, 137 are credit. They've also announced in that same report that 1.1 million merchants are now able to take chip cards, and that's up, increasing on an average about 23,000 a week. Okay, so that's one report.

The downside to that is that another competing survey came out from the Strawhecker Group that said, basically, if you've got about a million merchants enabled, that means that's only about 20% of the merchants that are out there. It's a cliché to say, but we've come a long way when it comes to implementing EMV at the issuer side and the merchant side. We still have a long way to go, especially when it comes to merchant acceptance.

Christine: You talked about the cost of the change, which is pretty clear. Is there anything else driving the pace of this implementation? Are there other factors that people are considering when making these decisions to migrate?

Steve: I think that it's going to become more and more clear as fraud numbers appear to be dropping. From some of those same announcements that were made by Visa and MasterCard, Visa looked at transaction volume from January 15, 2015 to 2016, and they saw fraud drop 18% at EMV-enabled merchants. That's a really big number considering there were not very many chip cards out there from January '15 to January '16. I think as people see hard numbers and the benefits that this is going to have of reducing fraud, hopefully it'll increase them to join in a little bit faster.

Christine: That's great, Steve. Thank you. Do you see any other challenges to implementation that we haven't spoken about yet?

Steve: You've got the basic problem where you have neither the merchant nor the bank ready to go, and there's not much you can do about that if neither of the parties are ready. I think one of the big challenges that we saw and I'm sure everybody experienced last fall during the Christmas shopping season was the education bump. Where people didn't know they had to use their cards, merchants/clerks were having difficulty explaining it, and then once you finally did get the card dipped in the right place, people were pulling it out too early and having to restart the transaction all over again. I really think we are over, for the most part, the education hurdle. Because most people, I think about 70%, have at least one chip card already in their wallet now and have probably gone through that initial hurdle of the ugly education in the checkout line of how to actually do this.

Christine: You mentioned the checkout the checkout line, and when I think about the EMV card, someone in front of me in line with an EMV card seems to take significantly longer to checkout than someone who doesn't. Is that potentially part of this hesitation from a merchant's perspective in terms of moving forward with this implementation? You can't get people through the line as quickly.

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

Steve: Yeah. I think that is one consideration. Especially, the larger the retailer the more you're looking at running as many people through the registers as quickly as possible. It's not your imagination. Another consulting firm out there, Harbortouch, did a study that confirmed what you all already knew. It takes seven to ten extra seconds to process a transaction using a chip card than it does using an old fashioned magstripe card.

Christine: Do you see that time dwindling over time? In terms of the checkout time, is there an opportunity for technological advances that is being worked on to rectify that problem?

Steve: Yeah. I think that'll speed up over time, and I think Visa and MasterCard have both issued some software fixes to eliminate a step or two to cut down on the transaction time. They just came out with those in March or April, so hopefully, we'll be seeing the whole consumer experience made a little bit smoother and quicker.

Christine: Fantastic. Steve, I wonder if you could talk about the differences between the chip and PIN model versus the chip and signature model.

Steve: Sure. I would say about 99% of the card issuers out there are going with the chip and signature or chip and choice model. That means you can use your chip card and then sign as opposed to using your chip card and using a PIN like you would with an ATM card where you need to enter a PIN to conduct a transaction. The general reason that banks favor just the chip is that the chip gets you 80% there or further when it comes to reducing fraud because it eliminates virtually all counterfeit fraud. PIN may eliminate fraudulent transactions if your wallet or purse is stolen. Someone wouldn't be able to actually use the real card and just sign for it. They'd need a PIN that, hopefully, you don't have written down on your card.

The question is at what level of security is it worth – is the benefit worth the added expense? For the vast majority of banks, they're just sticking with the chip and signature.

Christine: Okay. That's great to know, Steve, and I appreciate all of the input and insight that you provided for us today. We have a short timeframe that we're working with, so I wanted to open the floor up. There's a Chat window on the participants desktop. If anyone has any questions that they would like to pose to Steve while we have him, please enter those now, and we'll take questions for a few moments. It looks like I'm getting one already, just one moment. Okay. Steve, how would EMV impact online transactions where the chip can't be used?

Steve: Okay. That's the Achilles heel of EMV technology right now because there's not a widespread way to use EMV chip security in an online transaction. You'd still, for the most part, just be typing in the account number on the card. That's one reason why – the fraudsters aren't going away, but we're just going to be taking away one of their avenues to steal money by eliminating the counterfeit fraud channel for them. We really do expect to see fraud migrate over to online channels, so that's the Achilles heel. We're going to be plugging the dam in one place, but it's probably going to spring a leak when it comes to online transactions.

Christine: Okay. Someone's asking do you have any tips for the community banking base in terms of this implementation? Things the base should be thinking about in particular versus say a mega bank or a regional?

Steve: No. I think the first thing is probably – at least from the community banks that I deal with most of the time, is that you need to be loud and clear when it comes to whatever vendor you're working with and relying on to get you up and running. You want to make sure that they know what you want – first you have to decide what you want to do and what your plan is. Do you

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

want to switch or not? Okay. If you want to switch, how do you want to do it? Do you want to do it within a year? Do you want to do it within a quarter? Do you want to do it each month?

You need to present them with the plan so that then you can make sure that you're on their order list to make sure that you get the cardstock when you want it and when you need it and on time to implement your plan. It's the squeaky wheel gets the oil when it comes to the community bank and the vendor community. I'm sure you all know that.

Christine: A few more questions, Steve. In Europe, fraud has shifted to card-not-present. What steps can we take as an issuer to mitigate that type of fraud?

Steve: That is going to be really difficult. Because if a transaction gets compromised, the way it would get comprised to be able to be used online would be if your consumers use the magstripe. If you're chip-enabled – let's assume you're chip-enabled. The data that gets stolen is going to be from a merchant or a payment processor that is processing magstripe transactions. I think one way to encourage or to prevent this would be to encourage your consumers to use their magstripe on the card as infrequently as possible. Because when you use your magstripe, you're putting the information out there for a loss.

A lot of this is difficult. I know. If you think about it, what does the consumer care? I mean, they're going to get reimbursed. It's a hassle to get a card replaced, but they don't have skin in the game. The more you can encourage them to use the chip on their card and not the magstripe, that helps eliminate some of the vulnerability.

Christine: That segues into the next very interesting question, Steve. What do you think the impact would be if a financial institution would deny online transactions for their debit cards to avoid fraud?

Steve: I'd think you'd have a serious consumer service issue, and you'd probably have people leaving your bank.

Christine: Okay. That sounds about right. What about the idea where both the issuer and the merchant are both in compliance, but there's still fraud. Now where does the liability fall?

Steve: I believe that goes back to where it is right now, and that would be on the issuer if it's a counterfeit card. The whole idea is if you're using the chip, it's going to make counterfeit fraud a million-to-one shot. That's actually the ultimate goal is to have everybody race to the top when it comes to technology, and that should virtually eliminate transaction fraud in the chip world.

Christine: Great. What do you see – this next question. What do you see that doing in terms of the ATM? Is there any impact or effect on the ATM transactions?

Steve: Oh, good point. The liability shift for merchants was last October. Everyone realized that replacing ATM machines is a lot different than changing a POS device, so that was pushed back to a later date. Visa has made it October 2017 and MasterCard, October 2016. In about five or six months, if your ATMs aren't upgraded to accept chip card transactions, then you're going to be accepting the liability for counterfeit fraud, not the card issuer if they've upgraded their chip card. This is putting the banks in the position that the merchants are in now. One other thing that's the exception to the rule is gas stations have until October 2017 to change their pay-at-the-pump devices. Like ATMs, it was recognized that they're more expensive to replace than POS devices at a checkout line.

© Harland Clarke 2016. All rights reserved.
The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.

Christine: Thank you, Steve. Do you have any last words for this group? We're just about running out of time, and if there's anything that you wanted to close with, I want to give you the floor for just a moment.

Steve: No. I just want to say thank you very much. If you have any other questions, I think my contact information is on the screen. I work at ABA Center for Payments & Cybersecurity, and we cover a wide range of issues, and have a website that has a lot of good information. I encourage you all to check it out.

Christine: Thank you, and thank you so much again, Steve. You really provided some key insight, and we really do appreciate you sharing this perspective of the American Banking Association with us today. Jeb, I want to turn it over to you now.

Jeb: With that, we certainly appreciate everyone attending today. We do have a URL here that you can write down or type. It's pretty short. It's harlandclarke.com/aba-cpcp. It actually redirects to a page Steve has provided us. It has all kinds of great tools, so we recommend you go visit that. Thanks again for attending the Harland Clarke Audio Series. This concludes today's session.

© Harland Clarke 2016. All rights reserved.

The content for this series was created by Steve Kenneally from the American Bankers Association. The views and opinions expressed herein are those of the author, and do not necessarily reflect those of Harland Clarke.