COMBATING FRAUD

A REPORT BY CA TECHNOLOGIES AND PYMNTS.COM

PYMNTS.com

COMBATING FRAUD - TABLE OF CONTENTS

WHY 3-D SECURE IS PRIMED FOR IGNITION

It's not exactly breaking news that cardholder security is front and center of the payments ecosystem "to do" list. And, with that, the search for a solution that keeps cardholder data secure without compromising the consumer experience at checkout. Nowhere is this more important than online, where the incidences of fraud are increasing, and it becomes harder to authenticate the user.

One such solution, **3-D Secure**, was launched in 2001 to help online merchants reduce the incidences of fraud online. But, it's also fair to say that 3-D Secure didn't exactly meet expectations given the rather onerous registration process that consumers had to endure after the checkout had happened. As a result, this very robust and effective solution never really ignited as once envisioned.

That is all changing now as behavior-based authentication models leverage the 3-D Secure platform to do all of the important authentication work in the background, eliminating the onerous process once characteristic of this solution and positioning 3-D Secure as a robust tool in reducing fraud in an omnichannel world.

CA Technologies, co-creator of the 3-D Secure protocol uses behavior-based authentication models to examine the usual patterns of the cardholder, merchant and mobile device used to pay to authenticate the user (PC, mobile/tablet), which is critical given the seamless ways in which users move from device to device. These models are "smart" enough to reduce the need for secondary authentication.

CA Technologies Risk Analytics Regional Models are the brains behind this solution and are enriched using data from regional issuers. The secret sauce, though, is the data that is gathered from the devices the consumers use most typically when conducting transactions online.

These models use variables (a sort of mini-model) to isolate these behavior patterns. The variables may simply identify if the device being used is new, or the velocity of spending on that device or card is unusual.

The benefits can be enormous and the ROI compelling as a chart taken from this whitepaper points out. But, perhaps the best outcome of all is the reduction in the friction associated with the online shopping experience, and the number of declined transactions based on the new behavior of a consumer that is moving between devices more quickly than ever before.

This eBook is a combination of expert insights into how 3D Secure can help combat fraud in the payments ecosystem.

TEN THINGS NEVER TO DO WHEN DESIGNING A FRAUD SOLUTION

Revathi Subramanian

Senior Vice President, Data Science

CA Technologies

Cardholder security is very clearly at the front and center of the payments ecosystem "to-do" list. And with that comes the search for a solution that keeps cardholder data secure and curbs bank fraud. 3-D Secure, a protocol designed to help online merchants reduce the incidences of fraud online was designed to do just that. But 3-D Secure has often been criticized for creating too much friction into the process – putting the 95 percent of people who aren't the bad guys through the wringer instead of focusing on the 5 percent who might, in fact, be sketchy. CA Technologies, who is the co-creator of the 3-D Secure protocol, has addressed this by leveraging behavior-based authentication models to take on the important authentication work in the background, positioning 3-D Secure as a robust tool for reducing fraud losses in eCommerce transactions without subjecting consumers who just want to buy legitimately online with one big friction point.

Ten to fifteen years ago, ecommerce payments were rapidly multiplying. CA Technologies therefore co-created, with the payments networks, the 3-D Secure process, which provided a way for issuers to intervene and better understand card-not-present transactions. It started as an authentication solution, however, the 3-D Secure process has been criticized in the past with respect to the consumer experience.

"As banks used it more and more, the idea of intervening every transaction was not very palatable because the customer experience was suffering," said Subramanian. "There was money left on the table, which resulted from abandonment." There are three things that therefore must be balanced: the customer experience, the operational costs of customer abandonment, and the prevention of fraud.

"If you focus more on the few transactions that must be questioned and do not intervene on the remaining 95 percent of regular transactions, there's tremendous value for issuers," said Subramanian. But if every transaction is intervened, she added, issuers may end up losing 15 to 20 percent of transactions as customers abandon them. Significant revenue would therefore be lost. Achieving balance is the only way to increase card revenue.

HERE'S WHAT YOU NEED TO KNOW:

1. DATA: GARBAGE IN, GARBAGE OUT

If you look at the general data banks collects, said Subramanian, the quality is suffering – it is not collected uniformly. With respect to 3-D Secure, the way the data is collected is uniform. It's not data being dictated by the issuer, but rather directly from the merchant by request.

2. NO DOCUMENTATION, NO CHANGE

When dealing with data, one of the biggest issues that organizations have is that information is not documented the same way. With 3-D Secure, there's significant portion of the data created by a single entity. It's uniform and provides tremendous opportunity for issuers to bring data together. Device IDs called by the same name have a lot of value.

3. KEY EMPLOYEES ARE NOT A SUBSTITUTE FOR GOOD DOCUMENTATION

What ends up happening with banks is they'll change something or request something new in the fraud detection process, and it doesn't get documented properly. That piece of data, even though important, cannot really be used for awhile.

In 3-D Secure, she noted, you have a well-documented protocol. The pieces of information that come through for the merchant are fixed and well understood – there's opportunity to keep it uniform.

4. MORE DOESN'T MEAN BETTER

Rules are usually a requirement for any system, yet having too many rules can be counter-protective. A rules engine is a must-have to give flexibility to the issuer, and data driven rules are best. As 3-D Secure evolved, rules were applied based on unique data variables so that issuers no longer need to intervene in every transaction.

5. NEVER REST ON YOUR LAURELS

Because devices are growing and evolving, we need to constantly understand how they work. As fraud management systems get sophisticated, fraudsters also get sophisticated. Scoring processes have to keep on improving to tackle fraud effectively – and advanced analytical scoring is a huge value.

6. SCORE + RULES = WINNING STRATEGY

A sophisticated scoring system along with a limited set of rules to take into account operational considerations is the winning combination, said Subramanian. Scores tell you who might not be legitimate, and rules are what you decide to do with that knowledge.

7. FRAUD: IT'S EVERYONE'S PROBLEM

Every little bit of information we drop on the floor, every transaction that doesn't get recorded, every rule that doesn't get used right, every score that doesn't get used optimally, every fraud analyst that doesn't get trained well has an impact on the overall fraud management picture. 3-D Secure is a gold mine of information, and any bank that doesn't use an advanced scoring system using 3-D secure data is leaving a lot of cash on the table.

8. CONTINUAL ASSESSMENT IS THE KEY

It's important to assess the overall fraud management strategy in the context of the new information available through 3-D Secure. Data is power, especially when used to control risk. When more data becomes available, issuers should make use of it. They should continuously assess their whole fraud landscape and ask themselves what tools are available to them.

9. FRAUD CONTROL SYSTEMS: IF THEY REST, THEY RUST

3-D Secure has shown that it can have positive impact on fraud losses. According to Subramanian, strong models using the length and breadth of 3-D Secure's data (with a flexible rules system) can make it a key fraud control tool now and in the future.

10. CONTINUAL IMPROVEMENT: THE CYCLE NEVER ENDS

Every time there is a leap forward in the digital world, there is a leap forward in what fraudsters can do. This means that there must be a continual process of improvement among issuers – planning, doing, checking, and acting. It's important for them to use every bit of data that is available in complete fraud management strategy.

Today, 3-D Secure is dynamic and personalized. It targets high-risk transactions only, there is no up-front registration, and dynamic passwords provide enhanced protection. Equally as important, the cardholders and devices each have unique experiences that help issuers differentiate who is good and who is bad, arming themselves against fraud.

LOOKING BEYOND 3-D SECURE'S ROCKY PAST

Bob Stock

Strategic Partnerships, New Business Innovation
CA Technologies

Let's face it. 3-D Secure hasn't exactly won the eCommerce popularity contest over the last several years. Customers got confused when they saw pop-up windows, struggled with remembering passwords and then just said "never mind" at checkout. But 3-D Secure has come a long way. **Bob Stock, Strategic Partnerships, New Business Innovation at CA Technologies** spoke with MPD CEO Karen Webster about how 3-D Secure has moved past its "iffy" reputation to become a useful tool for eTailers to identify risky transactions more accurately and less disruptively.

Karen Webster: Let's talk EMV and the related aspects of security with respect to the EMV migration that the U.S. Is now facing. Since online commerce is growing rapidly, what solutions should be added to the retailer's security portfolio to mitigate the threat of online fraud?

Bob Stock: In other markets, specifically in the U.K., because skimming as a method of fraud at the POS has become difficult with EMV cards, the card-not-present fraud has spiked. We anticipate that to happen in the U.S. as it moves to EMV cards.

There are a number of things that can be done on all sides of the transaction. On the merchant side, they have a wide degree of sophistication, especially some of the larger merchants, about fraud detection, scoring, device identification, and more. They've put solutions in place to help them recognize suspect transactions, including things like 3D-secure, and that continues to advance.

On the issuer side, it's a bit of a challenge because when you look at e-commerce transactions, there's no connection between the issuer and the end-user on a given device. That is, the shopper is checking out at store A or B, but the connection used by the merchant to do device ID and other forensics is not available to the issuer. But issuers can certainly take a look at other fraudulent scoring techniques, and then there is a lot that can be done with 3-D secure.

Karen Webster: 3-D secure has kind of gotten a bum rap in the past, at least here in the U.S. I know the experience in Europe has been different because there really wasn't a choice for merchants. Why the stigma, and is the solution still relevant given the other things merchants are thinking about to prevent fraud?

Bob Stock: In the U.S., 3-D secure has been a bit less popular for a few reasons. One is that some of the U.S. e-commerce activities were pretty highly developed early on relative to other markets. For instance, Amazon became a sophisticated online merchant early on, and developed a lot of capabilities to use checkout and identify fraud.

Another reason 3-D secure didn't really accelerate was that the checkout experience and original intent of 3-D secure protocol was to provide an additional authentication for transactions, but the challenge with that was that, in the initial few years, every transaction and customer was treated the same.

Customers would have to enroll, if they weren't already, and select a password during checkout, etc. This led to more friction and higher shopping cart abandonment. That's the historical viewpoint.

A number of things, however, have happened to change that in the past few years. One of the key things on the issuer side is that providers have become much more sophisticated about enabling issuers to match the authentication requirement to the level of risk of the transaction.

So, because the 3-D secure protocol was designed to open a pop-up window, it's the only case where an issuer has a direct connect to the end-user's machine during an online transaction. That gives the issuer the ability to run device forensics, to see if the end-user is going through a proxy, and score all of these factors in real-time combined with the dollar amount of the transaction or the velocity against a machine, card, or merchant. They can use those things to tailor the user experience to the level of risk, even more so with added modeling.

They're seeing 97% plus transactions successfully go through without any change in customer experience, yet they still can identify fraud. That's a big change.

Merchants, too, see increase in e-commerce fraud, and in some cases are likely to run transactions through 3-D secure if there's risk evident. These instances have provided ways of leveraging the 3-D secure capability and technology in a way that isn't aligned with its perception historically.

Karen Webster: You mentioned modeling is helping to reduce friction. What are some the other things that really rest on the side of the card issuer to get over the hurdle of the misperception of 3-D secure?

Bob Stock: I think just being sophisticated about rules and modeling so that you can identify suspect transactions is one thing. The other thing we're seeing is that technologies are making it easy in the case of authenticating a transaction. Let's say a sophisticated issuer is able to pass 95 percent of transactions through. For the remaining transactions that show some sort of risk or are out of pattern, the authentication mechanism also has gotten much more advanced. Issuers can use a dynamic password or a one-time password generator as part of a mobile app, and can make it painless so a customer doesn't have to remember a password.

We've also seen instances where, in certain markets that are comfortable with second-factor security, mobile application programs have been used to ask the customer if they are in fact completing a transaction for a specific amount with a specific merchant. But overall, the most important thing that card issuers are doing is recognizing the risk and taking friction away for low-risk transactions.

WHAT A FRAUD SOLUTION LOOKS LIKE WHEN WE START FROM SCRATCH

Nick Craig

Worldwide VP Sales, Digital Payments

CA Technologies

In an interview with **Nick Craig, Worldwide VP Sales, Digital Payments at CA Technologies** and **Karen Webster, CEO at MPD**, Craig described how he'd design the ideal solution for stopping cyber criminals cold, and how some of the tools he'd use are right under everyone's nose.

KW: Before we get into what I know you want to talk about – fraud and security – now that we've seen Apple Pay, what is your reaction? How do you think it will transform payments?

Nick Craig: First and foremost, I think it's a fantastic announcement that was a long time coming. As to how it will transform the world we live in, I think the most important thing that we've seen is that clearly there's been a lot of focus on NFC as a method of payment. We think that's a great thing to encourage commitment to NFC as a platform, and the opportunity that then introduces. Introducing payment mechanisms onto millions mobile phones around the world is something we're all very excited about, and something we hope will act as a catalyst to drive mobile payments.

KW: I agree, I think there's been so much speculation about Apple, and now that we know, we'll begin to see a lot of interesting moves being made by different players in the ecosystem.

When Apple Pay was announced, Tim Cook made a very big deal about the secure aspect of the solution, and how card credentials were never going to be exposed to anyone at the POS, along with the tokenization of cardholder data being stored on the phone and being part of the transaction stream. What are your thoughts on their approach to keeping transactions secure?

Nick Craig: Our take on the Apple Pay announcement is that there were two use cases associated with the use of tokens. The first was where the Apple device was going to be used to complete a "tap and pay" payment at the point of sale. Apple stated that the Apple Pay system would use a one-time payment credential in passing the payment data from the mobile device to the merchant NFC terminal. We think that's a good thing in that it limits the availability of card data that can be leaked or compromised in the payment system.

The second use case that Apple mentioned was around the use of the mobile phone in the context of an e-commerce transaction. It's really unclear what exactly the user experience will be for e-commerce, but we believe that also represents an interesting opportunity and an impact on the way in which cardholders shop online.

I think tokenization has an important role to play in mobile payments, and we've incorporated tokenization in a feature of our mobile payments infrastructure. We're very excited that Apple is moving down that path, and it represents a great opportunity for the industry to take advantage of that.

KW: There's been so much discussed particularly, as the US is moving to EMV, as to how fraud will move to a card-not-present environment. There's been mixed reviews with respect to the available solutions in market today to address that. I know that CA Technologies is a pioneer in 3D-Secure authentication, which has had its own mixed reviews over the year. How do the various things we're hearing about – tokenization, 3D-Secure – work together? How are you helping your customers sort out this landscape?

Nick Craig: This whole space is obviously quite a complex ecosystem. Card-not-present has become a significant area of fraud, and as fraud becomes more sophisticated and developed, we've also seen the payments industry respond with those new initiatives. Tokenization, EMV, and 3D secure are just some examples that mitigate the fraud. What that means in the industry, particularly in relevance to recent breaches, is that cardholder data will become increasingly available to the fraud community. That makes it more difficult for issuing banks to identify the point of compromise, and easier for fraudsters to monetize that data they have with transactions that are reliant on card data alone. These card-not-present transactions represent such an opportunity for a fraudster.

What we are doing is ensuring that we focus on a couple of things that we think are significant in developing an effective fraud strategy. The first is to build adaptability into a fraud strategy. No longer can issuers look at this world, deploy technology solutions, and really be confident that those solutions will solve a problem for a period of time. There needs to be continuous improvement through the use of data, technologies and processes available. This means that treating portfolios in the same way becomes far less effective.

We're an advocate of ensuring that we built adaptability into the solutions we offer and put the issuer right at the heart of the decision cycle. It's about adaptability and control in a fraud strategy.

We also know the importance of data in fighting fraud. Issuers are continuing to seek deeper insights to allow better understanding of fraud and the threats they've seen. Having this flexibility to act quickly sounds simple, but for lost of systems and processes today, that flexibility is difficult to achieve. What we focus on is allowing issuers to achieve greater levels of adaptability and insight to put them at the heart of the decision process. In particular, the work we're doing around authentication models is a very exciting opportunity to combine a couple of those elements to deliver solutions that really do attack the card-not-present fraud problem.

Karen Webster: CA Technologies' neural network authentication models sound very interesting, and potentially very useful to card issuers. How do they work?

Nick Craig: The first thing to understand is that this really is the first time that artificial intelligence and these advanced techniques are being applied to the world of authentication. And that's important because authentication itself offers a unique opportunity.

When you think about the world that we live in and the fraud prevention solutions deployed to issuing banks over the years, on the authorization side, those systems are working with very limited data streams that largely have not changed in many years. Authentication brings new digital data that can be leveraged, so for instance, you're able to see the device the cardholder is using, the location of that cardholder at the POS, the connection speed that they're connecting over, and each of those provide an affective variable when compared to traditional data streams that we're used to seeing – transaction amount, currency, merchant details, etc.

There's a set of capabilities that we are deploying to map both the genuine cardholder behavior as well as the fraudulent behavior. Historically, the focus has been more on trying to map fraudulent behavior to predict future instances of fraud occurring again. But the combination of the data with advanced techniques allows us to provide a significant opportunity to issuers in fighting fraud.

Karen Webster: As a consumer, the first time that I transacted on a German fashion site that I'd never visited before, I was sure that I'd have my transaction declined because it was totally out of pattern for me. But it went through just fine. Around the tenth time I went to that site, however, my transaction was declined and I got an alert from my issuer asking if I was really attempting to make that purchase. Why would the first time have been okay, but the tenth time not okay?

Nick Craig: If you think about what we are doing, ultimately we want to separate the fraud from normal behavior. When we look at normal behavior, we are mapping it at a detailed level. We're not just looking at whether or not this is Karen, if she's using the normal credit or debit card that she typically uses, is she shopping at the same merchant that she usually visits. It's those additional data points that provide opportunity to get the broad perspective. We're identifying deviations from your normal behavior by looking at pivots in data elements, and how the connection speed versus the card versus the merchant interact together. That's why, perhaps, in your situation, if the solution behind the scenes is trying to map fraudulent behavior, there might be something like the value of the transaction, time of day, or the merchant itself that triggers the riskiness of the transaction.

What we're doing is matching the fraudulent behavior with the genuine behavior, and the combination of those data streams with sophisticated techniques that we're using give us that opportunity to reduce those instances where your shopping experience is impacted because the transaction is declined. That's really what's behind the scenes.

KW: It seems to me that this is something that should be a typical part of the fraud strategy for an issuer. Why isn't it, and what are those individuals or companies leaving on the table by not incorporating this strategy?

Nick Craig: I think issuers certainly are doing more of this. What we're seeing, with the introduction of our advances analytics models, is that this is providing a significant opportunity for banks. It's not that they're not using them, it's just that there's a new set of technology there that they can now take advantage of. Speaking to the value itself, obviously the most immediate benefit for the card issuer is reducing the net loss and improving fraud protection.

An affective fraud solution is going to really need to improve the balance between fraud and customer experience. It's very easy to reduce fraud – just decline lots more transactions. The consequence of that, however, is that the customer is not able to shop without getting frustrated. That has a big impact, causing lost revenue and, more importantly, lost loyalty.

Consumers now have increasingly different options for payment methods, so it is becoming important for banks to not only make sure that they're offering the best customer experience, but also that they're securing that front-of-wallet status so that consumers always continue to use their card. As customers decide and create preferences, it's very difficult to change people's minds, moving them from one payment method to another. The other thing that's often overlooked is the operational impact. Clearly there's a big revenue opportunity in allowing customers to shop online more frequently and easily, and to reduce fraud. There's a very significant ROI that comes with these types of solutions.

KW: If you had a clean sheet of paper, and you were asked to design the optimal fraud solution, what would it look like?

Nick Craig: I think the principles we've talked about are very important. It's about going deeper into the data and understanding it, looking at it from a multichannel perspective across the entire organization. Also, the adaptability that we talked about – building and designing systems not just from the standpoint of delivering a result, but from the standpoint of knowing that, in the future, it's likely to change. Putting that control in the hands of the issuer to be able to develop and continuously evolve their strategies is key.

Karen Webster: I think people think about card-not-present transactions as those that we're initiating from our computers or mobile devices when we're shopping online. But as we've witnessed with Apple Play and other players over the last few years, the ability and cloud-based digital solutions to transact in physical stores will only create more of an environment for CNP transactions to evolve and scale. These kinds of things will only become more important.

Nick Craig: Completely. And when we also think about how quickly things move, industries change, and opportunities emerge, and the existing systems that banks run today, the challenge is a consideration of these existing systems and investments that have been made. It's much more about openness, adaptability and integration, rather than silver bullets that solve all of the problems, which we know is not the way of the world.

ONLINE TRANSACTING IS SAFER THAN A CARD PRESENT WORLD

Revathi Subramanian

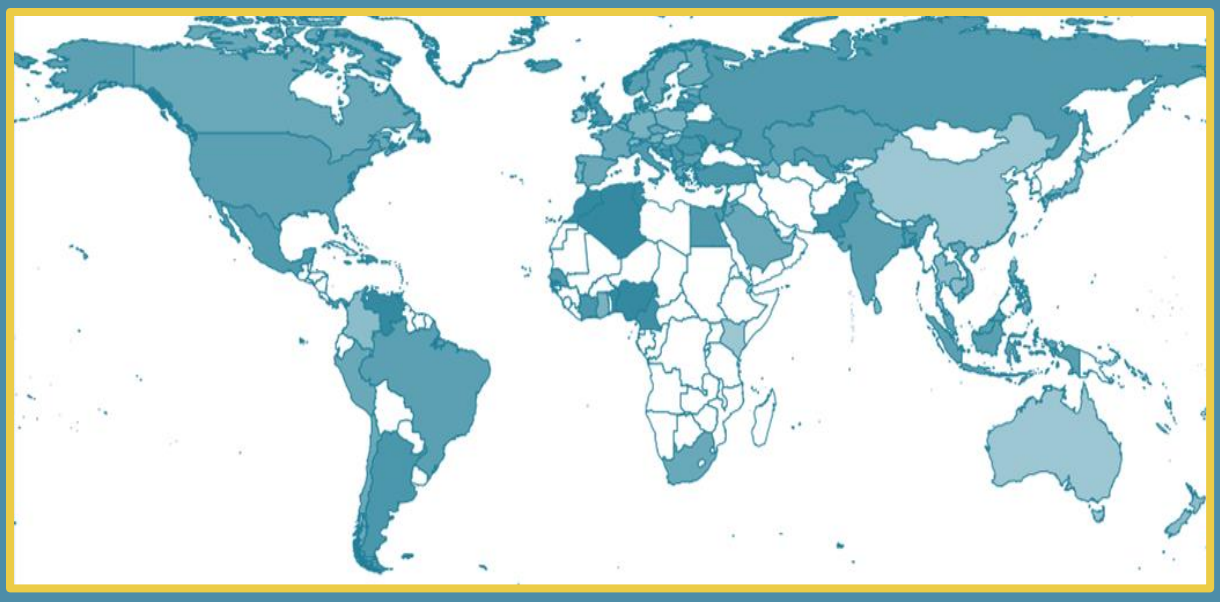
Senior Vice President, Data Science

CA Technologies

Revathi Subramanian, Senior Vice President of Data Science at CA Technologies conveys that online transacting is safer than a card-present world, in an interview with **Karen Webster, CEO at MPD** surrounding the state of online fraud around the world. Subramanian said that we have the data, the models and the tools – right now – to make online transacting safer than offline. But, they're just not being used.

E-COMMERCE FRAUD AROUND THE WORLD

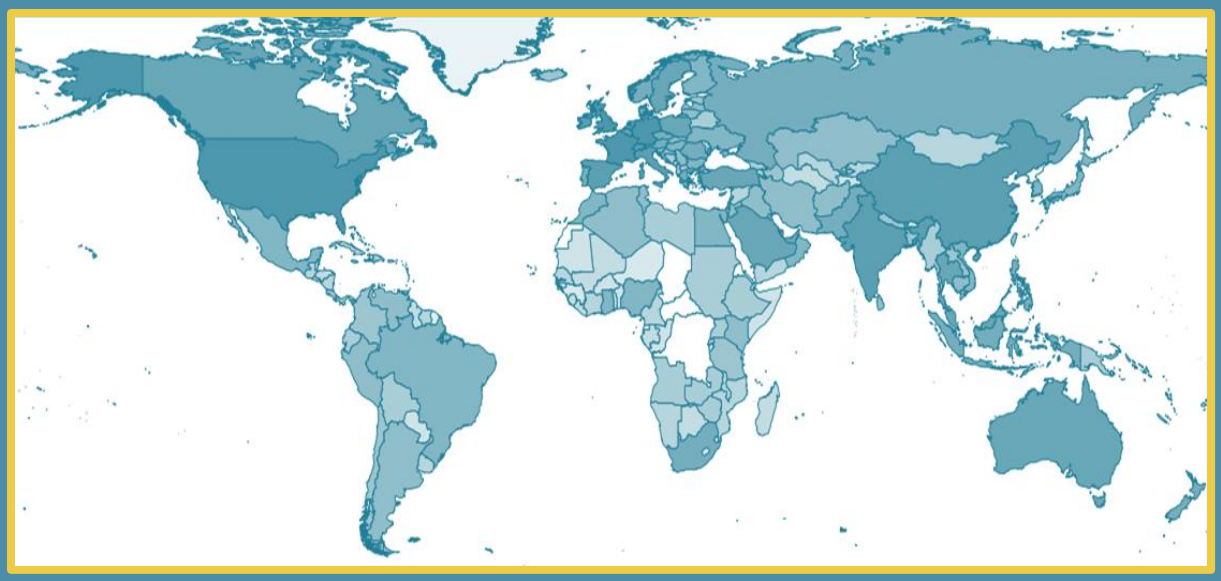
CA Technologies indicates where online fraud occurs in the world, with darker areas having the highest numbers of fraud.



E-commerce trends, said Subramanian, are shaped globally, and with each transaction comes a goldmine of information not available in the regular authorization stream. Device configuration and location, as well as browser characteristics, IP addresses, and more can be used to understand where and how fraud is happening.

Where Transactions Are Happening:

The below chart shows where online transactions are occurring around the world, with darker areas having the highest numbers.



THE BIG DATA OPPORTUNITY

The 3D Secure protocol gives the issuer the change to peer into a transaction as it is happening, and gather information on it. It has reached critical mass and continues to grow in use and popularity. In addition, detailed unique data about the customer's internet shopping habits including the device used, location, merchant URL, connection speed, type, the anonymizer, is available.

Data-driven techniques are proven in authorizations but have a card present view in terms of data. But, noted Subramanian, information available for card-present transactions doesn't even come close to the level available for online transactions. Advanced analytics with a Big Data infrastructure can therefore pave the way to creating tremendous value – and reducing fraud – to actually create an environment where it is safer to transact online than with a physical card. "The reason we might be safer with online transactions as opposed to card-present transactions is because we have the ability to use the information available with advanced analytical systems," she said.

Advanced analytics with Big Data infrastructure allows companies to detect fraud better while impacting fewer transactions, improve customer experience and create value for issuers, create customer insight and learn about the customer.

According to Subramanian, there's tremendous benefit to using 3D Secure for merchants, issuers as well as consumers. Below is a chart showing transaction data in black available in the regular data stream, with elements in red only available with a 3D Secure solution.

WHAT IS 3D SECURE?

Subramanian went on to explain that 3D Secure provides a mechanism to allow for the authentication of the user in real time at the point of sale online. She further stated that this provides improved visibility and control to the issuer for the purpose of fraud prevention along the following parameters:

Real Time Authentication: A mechanism to proving the identity of a cardholder while shopping online where traditional POS measures (chip & PIN) are not possible.

Device and Transaction Location: Provides valuable insight to the digital world allowing data to be seen not possible at authorization, i.e. device ID & geolocation.

Transaction Data Available When a Merchant Prompts for 3D Secure

"If a 3D Secure solution is deployed, all of this information will really be fair game," said Subramanian.

CA TRANSACTION MANAGER

- PAN
- Merchant ID
- Merchant Name
- Merchant URL
- Merchant Country Code
- Transaction Date (Actual)
- Transaction Time (Actual)
- Transaction Amount
- Transaction Currency
- HTTP Header Information

CA RISK ANALYTICS

OBSERVED

Customer's:

- Operating System
- System Language
- Time Zone Offset
- Monitor Details
- Browser Details
- Plug-ins
- IE Plug-ins
- Camera/Microphone
- Fonts
- Network IP Address
- Connection Type
- CPU Model and Clock Speed
- Volume of Boot Partitions
- True IP Address of End-User

CA RISK ANALYTICS

DERIVED

- Zone Hopping
- User Velocity of Card Use
- Device Velocity
- User Previously Associated with Device
- New User or New Device
- Device Known, But New User at Device
- Merchant Velocity
- Negative IP
- Negative Device
- Trusted IP
- Trusted Device
- End-user geo location
- Anonymizing Proxy Check

*Data in **orange** is only available with 3D Secure*

THE VALUE OF 3D SECURE

Subramanian was asked a somewhat rhetorical question during the discussion: "When we talk about the value of 3D Secure to the real constituents in payments, does the merchant feel like it's a worthwhile tradeoff?"

Her response points out that if the issuer, for example, collects all of the information and still chooses to authenticate, the abandonment will still be rare. The merchant and issuer will lose the transaction, and it's not a desirable solution for the merchant. They don't have the fraud liability, but they are losing a lot of the transactions if the issuer decides to do a password check.

According to Subramanian, "The merchants actually get to gain a lot from this if the data is being used very effectively." For cardholders, it will reduce friction and make shopping safer, for merchants, they will benefit from a liability shift to the issuer, and for issuers, they will get tremendous customer insight.

But is this costly for the issuer to implement? "No, not really," said Subramanian. "Even if you have a few merchants using your card, the liability is still on the issuer. If the issuer does not implement the 3D Secure solution, they end up losing."
The true value of 3D Secure to issuers is that it creates frictionless customer checkout and increased revenue, isolates true fraud from non-fraud, and decreases operational costs.

"There is much higher revenue loss when you're allowing transactions to be abandoned by intervening in a large percentage of the transactions," said Subramanian. The data therefore needs to be used more effectively and intelligently.

WHY MODELS?

Subramanian is a big believer in models, and talked extensively about CA Technologies patent-pending neural network authentication models that provide the "ideal combination of predictive power, stability and flexibility for e-commerce fraud detection."

The models utilize data described earlier and extract features with state of the art analytic techniques, uncovering behavioral insights on multiple pivots. At the same time, the models reduce fraud and customer friction and provide unparalleled flexibility to the fraud manager.

But the models have to be extraordinarily sophisticated, noted Webster, because we're in a very mobile society. Consumers are getting new connected devices and transacting all over the place, even on airplanes. So how are issuers being served this insight, and able to make decisions that go with the flow?

WHY NEURAL NETWORKS?

That's why Subramanian says that neural networks offer the ideal combination of performance, flexibility and feasibility, for very large mixed-type behavioral systems. She said that "there are no distributional assumptions on input data, and you can also get "state-of-the-art performance on even the most non-linear data." Finally, there is a linear training time and constant scoring time regardless of the size or complexity of the input data "What we are really doing is associating bad behavior with characteristics and how the correlate amongst each other, for each particular cardholder and so on," said Subramanian.

CA Technologies' neural network authentication models are powered by advanced machine learning techniques, understand legitimate and fraudulent behavior in context of the individual cardholder, and are updated in real time. In addition, said Subramanian, they provide greater accuracy and stability and produce a meaningful granular score.

"I really think the special sauce that CA Technologies has is the specific data we have and how we configure it in a specific combination that we use in the neural networks," said Subramanian.

Providing Issuers With a Better View

Subramanian said that CA Technologies is able to keep track of the location, device DNA, behavior, and history of a specific device being used to transact.

CA RISK ANALYTICS

Where is the user?

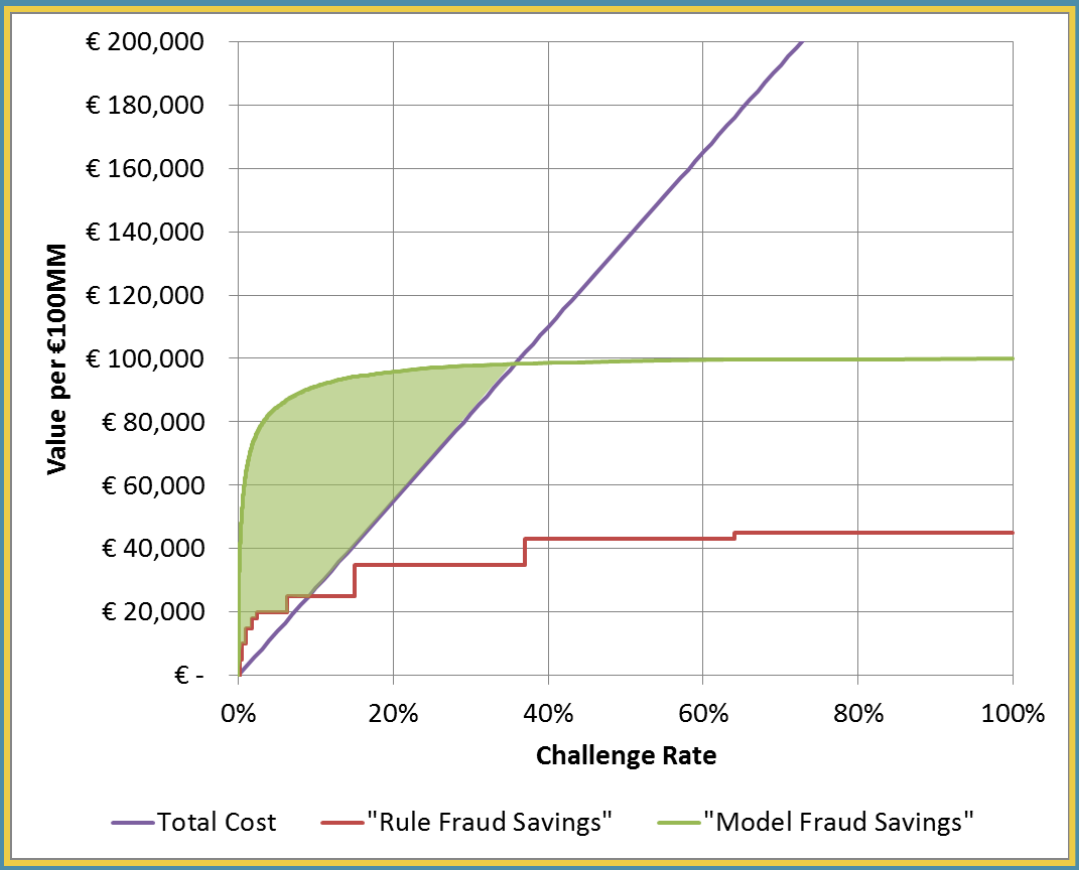
What device is being used?

What is the user trying to do?

Is the action consistent with history?

LOCATION	DEVICE DNA	BEHAVIOR	HISTORY
▪ Is the location inherently suspect? ▪ Have they been there before? ▪ Where were they recently?	▪ What kind of device is it? ▪ Have they used it before? ▪ Has it changed since they last used it?	▪ Is this a typical merchant type for the user? ▪ Is the action inherently risky? ▪ Have they done similar actions before?	▪ Is this a normal time of day for them? ▪ Is their frequency of login abnormal? ▪ Is their current action consistent with prior actions?

THE IMPACT OF A MODEL ON FRAUD



Subramanian walked the audience through the impact of a model that has been implemented. "What's represented in green is the model performance that we've seen. If the fraud losses are about 100,000 euros, and really all that you want to do is authenticate a small percentage of transactions, well-over 80 percent of your fraud can be contained within that," said Subramanian. "You've improved customer experience and fraud detection, while increasing the interchange and interest rate for the issuer and not abandoning transactions and eating into the merchants' profits."

Models can therefore provide the best of both worlds – maximize detection and minimize customer impact (cost). And because they are constantly updating and processing data, the actual building of the model itself takes only a few months to do, said Subramanian.
Her point, in other words, is that the essence of what the neural network provides the issuer with the ability to do is minimize the friction and maximize the revenue opportunity.

"In order to truly learn from cyber attacks, we cannot expect people to report a fraud attack, and then proceed to understand it. That seems to be the approach that a number of folks in the space take – we question how affective that is," said Subramanian. "We want to understand fraud as it is happening."

In the future, she added, these authentication models "will become a requirement in this increasingly online world."

HOW MOBILE SHIFTS THE PARADIGM OF PAYMENTS AUTHENTICATION

Doc Vaidhyanathan

VP Product Management, Digital Payments

CA Technologies

It's hard to imagine life without the smartphone. Mobile devices are now being used to complete the shopping process online and in stores – and 94 percent of us actually sleep next to them. For merchants, it's that personal connection to the consumer that provides a critical sales channel, and an entirely new way to look at how we authenticate consumers as part of the commerce experience. **Doc Vaidhyanathan, VP Product Management, Digital Payments at CA Technologies** caught up with **MPD CEO Karen Webster** to get into the specifics on this authentication revolution in an expanding world of mobile commerce.

MOBILE: THE NEW WAY TO AUTHENTICATE THE CONSUMER

The mobile revolution at first began without making a serious splash – gently, with the introduction of the Blackberry and later the iPhone, and consumers began to see the benefits of these technologies. This revolution has since prompted CA Technologies to completely rethink the payments authentication process.

So how does mobility build into authentication? Right now, we think of authentication traditionally as a way of identifying who you are, and its companion is something called "authorization" – figuring out, after your identity is determined, what you're allowed to do.

According to CA Technologies, there are three main parts to traditional authentication – 1) something that you know, like a password; 2) something that you have in your hand, like a token of some sort that generates a code; and 3) something that you are, like a fingerprint or eye scan.

"**The mobile device** brings together something that you have, the device, and something that you are, like a fingerprint, and even in some cases something you know, a password," said Vaidhyanathan. "At one level, the mobile device is beginning to blur the difference between all three."

So is our mobile device really separate from us, given our close relationship with (and in some cases, reliance on) it?

But what other attributes of the mobile device make it attractive, asked Webster, besides the fact that we're addicted to them?

What's so unique about the mobile device, said Vaidhyanathan, is something everyone has. It's caught the world's attention in terms of the speed of its global adoption. This device is also their own – it's not something that's shared. All of a sudden, their phones can identify them. And most people have just one.

The fact that these mobile devices are not shared creates a huge opportunity in the world of authentication.

"Now there's one-to-one correspondence between every person and a phone. That's an amazing thing," said Vaidhyanathan.

The three ways we can use mobile devices to authenticate include:

1) Authenticating oneself **with** something else using a mobile device.

2) Authenticating **to** the device – getting access to the device using a fingerprint or something else.

3) Authenticating **through** the device – if the person's bank or enterprise wants to do a voice or facial recognition, for example, the mobile device can be an instrument.

"The fact that there are these three varieties of authentication allows you to mix and match, and create the right level of authentication that you want," said Vaidhyanathan. The other dimension that you have, he added, surround the types of authentication schemes.

Consumers use several devices during the course of their life, each of which is in some sense giving them access to something. For example, a boarding pass is a method of authentication getting a traveler access to the gates at an airport. Things like boarding passes and hotel room keys are meant to grant people access for one or a few days. Work badges or debit/credit cards, however, are valid for years, and driver's license numbers are valid for a lifetime, as well as thumbprints.

"The beauty of the mobile device is that one device is able to support all of these things, whether it's something that will change frequently or last a long time," said Vaidhyanathan.

"What is interesting about the mobile device is that all of these components can sit in the device itself. It's not only a credential, but it also includes all three components – that's a phenomenal situation to be in," said Vaidhyanathan.

WHY USE MOBILE DEVICES FOR AUTHENTICATION?

The advantages of using mobile devices for authentication include being able to manage the entire provisioning process using the device. The second benefit is something called "multi-mode usability." A typical credential has only one mode in which it's used – it's something that's scanned, swiped or visual. With a phone, the same thing can be rendered in multiple ways – whether it's visual, interactive or automatic. Lastly, with a mobile device, there is the ability to retain usage history, which makes a user audit possible.

Provisioning integration through apps: the same device used through entire lifecycle.

Multi-mode usability: visual, interactive and automatic.

Retention of usage history: user audit is possible.

"Traditionally, authentication has been thought of as a way to grant the legitimate users access and keeping away the fraudsters. What mobile and increased mobile usage does is change the paradigm," explained Vaidhyanathan. "Users ask, if they are prepared to share more information about themselves, can they get access to more things? Can they get faster access?"

By 2018, there will be over 1.7 billion consumers with smartphones, according to a Statista report. User location will become available for authentication. That will make it such that using a fingerprint or biometric technology via mobile device is the standard for security and authentication – it will become "human-factor friendly."

"What the mobile device will let people do is to continue using their devices when they go to work, to the bank, to the airport, and other places, and the phone will figure out how to authenticate everything it needs to," said Vaidhyanathan. "It will become easier from a perspective of authenticating."

Webster then asked, would consumers see having a phone be that tied to authentication and security as risky?

There will be a certain set of people who want to be off the grid, untied from their devices. Mobile authentication and security isn't for everything – enterprises will accept that some people won't want it, said Vaidhyanathan. But newer generations – millennials and those coming after them – are born with mobile devices integrated into their lives. They will get more comfortable with this idea of mobile authentication, especially in return for getting certain access and privileges and ease of operation.

According to Vaidhyanathan, new enterprise applications for mobile include:

1) Replacing "plastic" badges to open doors, i.e. at hotels

2) Proximity authentication via mobile – access to laptops

3) Providing "tap and pay" to customers – NFC payments

4) Biometrics – facial recognition or wearables to allow access

MOBILE WALLET: THE PROMISED WORLD?

The evolution of the mobile wallet has gone from the process of swiping a "mag-stripe" card through a reader, to inserting a chip card and entering a PIN, to tapping a mobile device like an iPhone 6 at an NFC reader. Largely due to Apple Pay, NFC is becoming the standard for mobile payments.

But in order to use mobile as a payment card, said Vaidhyanathan, the following sub-systems must be in place:

Provisioning: Personalizing and setting individual card details, verifying user and device

Making payments: Rapid and easy "tap to pay" experience

Back-end infrastructure: Authorizing new payment method/messages

To effectively carry out these processes, enterprises can deploy strong authentication solutions like the CA Mobile OTP for Payments.

CA Mobile OTP for Payments:

1) Reduce fraud losses

2) Simplify authentication

3) Dynamic OTP technology

4) Utilize across multiple channels

5) SaaS capability