WHITE PAPER | OCTOBER 2014

3D-Secure Authentication using Advanced Models

Models used for risk- and behavior-based authentication of eCommerce transactions can reduce losses and provide frictionless checkout for low risk transactions.

Paul Dulany
Hongrui Gong
Kannan Shah
CA Technologies, Advanced Analytics and Data Science

Table of Contents

Executive Summary

Challenge

Issuers need to balance eCommerce payment transaction security and a smooth customer checkout experience. The crux of the matter is how to provide a seamless checkout experience for legitimate customers so they won't abandon their transaction or use a different form of payment while at the same time stopping illegitimate attempts to transact. The use of behavior-based authentication to determine which transactions should be impacted by requiring the customer to go through additional means of authentication is critical for reducing customer friction while creating better assurance that the transaction is legitimate. Rules are an important component when providing this risk- and behavior-based authentication. When models are added, and used to guide the application of risk-based rules, the impact upon illegitimate authentication attempts can be greatly increased while the impact on legitimate customers is decreased, providing a better experience for the cardholder and loss reduction for the issuer.

Opportunity

The 3D-Secure channel presents many opportunities for issuers. With the significant increase in eCommerce fraud, combined with the liability shift, 3D-Secure authentication provides a first line of defense for issuers. However, it is important to utilize that first line of defense wisely and to the best advantage. CA Risk Analytics provides the opportunity to examine eCommerce transactions during authentication using unique information not available to authorization fraud detection systems, and to thereby prevent an illegitimate transaction. An assessment of authentication risk must be made in order to provide an uninterrupted checkout experience to the majority of legitimate cardholders. With CA Risk Analytics in place, issuers can reduce losses and limit customer friction.

Benefits

CA Risk Analytics can help issuers evaluate the risk level of online activities at 3D-Secure merchants. It transparently assesses the risk that an eCommerce transaction is being attempted by someone other than the legitimate cardholder, in real-time. It can identify a significant portion of legitimate transaction attempts and allow customers to continue with their purchase without impact while similarly identifying illegitimate transaction attempts that should be stopped. Device identification, geo-location, connection characteristics, and historical patterns can be used to assess the risk of each attempted transaction.

A critical aspect of CA Risk Analytics is the availability of advanced regional models that evaluate the risk level of a given transaction attempt using sophisticated analytics, including a behavioral neural network model, and provide a score that indicates the riskiness of that attempt. Rules within CA Risk Analytics may then combine this model score with other business factors to determine the best treatment of a given transaction attempt, resulting in a significant increase in the effectiveness of the solution.

Section 1

3D-Secure Provides the Basis for eCommerce Loss Reduction

The 3D-Secure protocol provides issuers with many opportunities that must be used to get the full benefit from and protection afforded by the 3D-Secure channel.

The 3D-Secure channel focuses on authenticating eCommerce transaction attempts. It is important to understand the difference between authentication and authorization. Authentication is attempting to confirm that the person initiating a transaction (or other activity) is the legitimate and genuine cardholder. Authorization is attempting to validate that the (confirmed) cardholder has the authority to transact (based upon policy, available balances, account status, and other concerns). Please note that fraud can occur and be detected in both the authorization and the authentication steps, but there are key differences; for instance, authentication does not directly counter first-party fraud. However, regardless of the fraud type, authenticating the person attempting a transaction is the starting point for ensuring that the transaction itself is valid.

For Card Present transactions, the physical presence of the card has long been accepted as a key component of authentication. As illegitimate users became more sophisticated, issuers responded with better security on the cards (magnetic stripe, CVV/CVC/CID, and smart cards). These data, or the results of authenticating with this data, are generally sent through on the authorization request.

For Card Not Present (CNP) transactions, physical authentication via the card is no longer possible, and generally the liability has been on the merchant. However, with the advent of eCommerce, it has become necessary to develop robust authentication of eCommerce transactions. The data on the authorization request, while sufficient for authorizing a transaction, is insufficient for authentication of an eCommerce transaction. Therefore, the 3D-Secure transaction was born, with different information than the authorization request and designed for authenticating the person attempting to make a transaction. This task, which is fundamentally different from authorization, requires a unique perspective. However the results from this authentication can be utilized in the authorization stream to provide a better context to the authorization system.

To be explicit, when we refer to fraud in this document we mean authentication fraud on eCommerce 3D-Secure transactions.

Using the 3D-Secure protocol, there is the opportunity to examine eCommerce authentication attempts, using unique information not available to authorization fraud detection systems, and to thereby prevent an illegitimate transaction before it creates an authorization request. When using the CA Risk Analytics system, this unique information includes a unique ID for each device (Device ID), a URL being accessed by the cardholder to make the transaction (Merchant URL), the current IP address of the device, and auxiliary information from third-party data providers including device location, connection speed, type, and anonymizer identification, as well as other information. This information significantly augments (but does not replace) the traditional information such as the amount, currency, merchant name and ID, card identifier, and other information. With this augmentation, 3D-Secure authentication models can provide more benefit than authorization models that only see the traditional information, providing strong detection of illegitimate authentication attempts while impacting only a small portion of legitimate attempts.

The 3D-Secure channel provides information in real-time for analyzing authentication transactions, in particular, we have the opportunity to update information regarding the card, device, or other pivotal entities in the transaction in real-time. This allows any following transaction to reap the benefit of increased information and context when it is evaluated for authentication risk. This can be especially powerful when looking at entities across banks in a cloud SaaS environment.

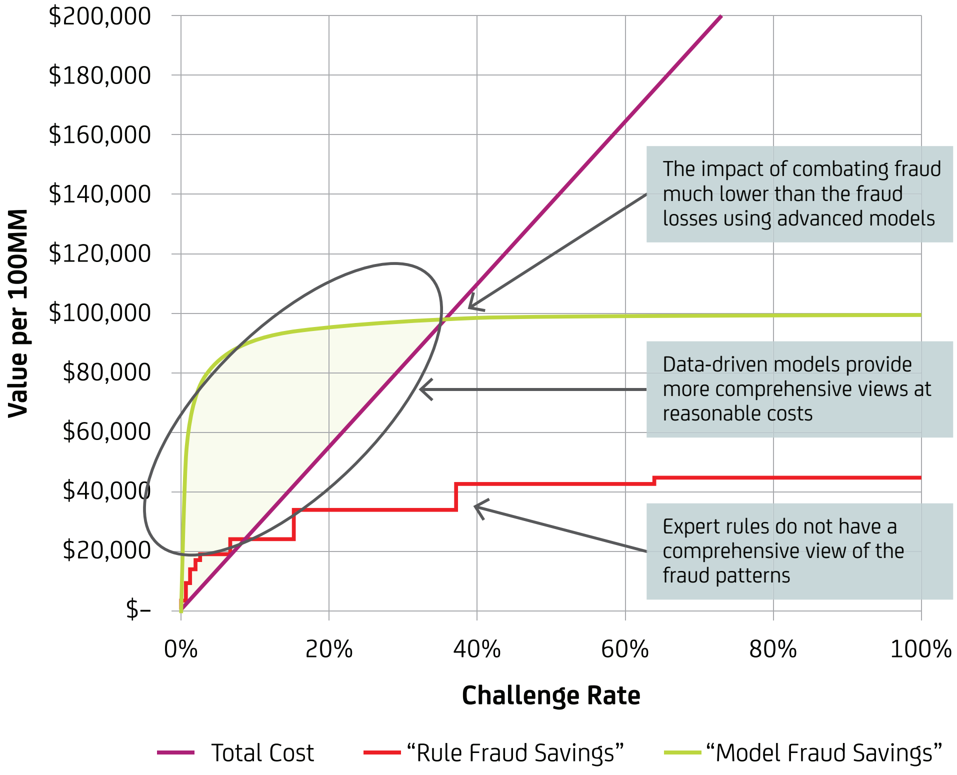
There is also the opportunity to make eCommerce shopping relatively frictionless. Early 3D-Secure implementations present challenge questions to all purchasers at 3D-Secure merchants. If the challenge is strong, such as using one-time-passwords (OTP), then this can be reasonably effective; if the challenge questions are weak, such as asking for information needed to perform the transaction itself (expiry date or CVV2), then this does little to combat losses. However, there is a secondary effect: presenting cardholders with challenge questions introduces "friction" to the transaction—increasing resistance to completing the transaction and negatively impacting the customer experience.

The negative impact of friction on customer experience is not purely qualitative—it has a quantitative component too: it increases abandonment and "false failure" rates significantly. Abandonment results in lost interchange fees as well as larger impacts such as the loss of revolving balance for credit cards, or possible customer attrition, which is a significant issue for both debit and credit accounts. These impacts allow one to quantify part of the impact to issuers of a negative customer experience, and provide a strong motivation for reducing the friction of the transaction. In the extreme case of challenging all customers, the costs of abandonment can outweigh any possible loss savings. Therefore, it is critical to evaluate the risk of a given transaction and intervene in the process only when well justified. This is best done using behavior-based authentication.

Figure 1, on the following page, shows an example of the total cost of fraud detection (including lost opportunity due to abandonment) (the purple line), the savings of typical rule system (red line), and the savings from a typical CA Risk Analytics Regional Model (green line). Note that as the Challenge rate increases, so does the cost of operating the system. With a rule system, which typically doesn't have a comprehensive view of the fraud, the cost of operating the system can quickly overwhelm the savings from the rules. With an advanced data-driven model, a comprehensive view of the fraud can be accomplished at a reasonable cost. The green shaded region shows the advantage of a model over rules.

Figure 1.

The total cost of fraud detection.



The impact of combating fraud much lower than the fraud losses using advanced models

Data-driven models provide more comprehensive views at reasonable costs

Expert rules do not have a comprehensive view of the fraud patterns

Section 2

Behavior-based Authentication

Behavior-based authentication involves looking at the current transaction within the context of usual patterns of cardholder, merchant, and payer's device activity to see if this information alone can produce a strong confidence that the payer is the authentic cardholder. If so, then there is no need to bother the payer in the middle of their transaction, and the transaction can go through without impact, significantly reducing friction and the likelihood of abandonment and thereby improving cardholder experience[1]. Alternatively, if there is a strong confidence that this is not the authentic cardholder, then the transaction may be outright denied, thereby preventing an authorization or settlement request and eliminating the chance of fraud altogether even if the fraudster knows authentication information. Finally, for those transactions where there is neither a strong confidence for legitimacy nor for illegitimacy, then moving to a strong authentication interaction with the cardholder may be advisable. The key idea in behavior-based authentication is to utilize behavior patterns to reduce the uncertainty regarding whether or not the person attempting to authenticate is the legitimate cardholder, and therefore simultaneously (a) reducing the portion of legitimate transactions impacted by secondary authentication, while (b) ensuring that more frauds enter secondary authentication and (c) outright denying more frauds.

Models as behavior-based authenticators

The CA Risk Analytics Regional Models are built using data from regional issuers who allow their data to be used in the CA eCommerce Consortium and who contribute “truth data”[2]. These data include both credit card and debit card 3D-Secure transactions.

Regional models encompass a number of different elements. First, the models utilize information from the current transaction. This includes the date and time, amount, location of the person attempting to authenticate for a transaction (the cardholder’s computer or mobile device in the case of eCommerce), merchant name, id and URL, information regarding the device’s IP address, connection characteristics, and auxiliary information from third-party data providers. This information is critical for the model to understand the current transaction. However, it is not enough for an understanding of the behaviors involved.

Second, the models utilize information from previous behavior for the pivotal entities of the current authentication attempt, such as the card, device, or merchant. Information from past behavior is distilled into the important factors for looking at behavior patterns. These include information such as: which merchants have been visited, the amounts, locations, and devices used for each of these visits, and which unique devices have been used with this card. Similar patterns are looked at on other pivotal entities as well. These “pivot distillates,” as the histories are called, are updated upon each observed attempt to authenticate for a transaction.

Third, the models utilize complex variables, including mini-models, that isolate the behavior patterns of the pivots involved in the transaction as well as determining how and if the current transaction fits into those patterns. These variables may be as simple as identifying if this is a new device for use on a given card or the velocity of spending on a card or device. However, they can also be complex, comparing the tendency for a given cardholder to do repeat shopping and the number of times they have visited this merchant to the same patterns for other people.

Fourth, the models utilize tables built using historical data. These tables provide information on past tendencies for legitimate and fraudulent transactions in the historical data, including trend and Naïve-Bayesian metrics.

Finally, all of these different elements are presented to a non-linear numerical model that weighs their different predictions regarding behavior anomalies and the risk of illegitimate attempt. These models capture the non-linear behaviors: important relationships between variables and the likelihood of fraud that are not a simple linear relationship. They compare risky indicators with mitigating factors (this is a high-fraud merchant in a high-fraud amount, but this person has done this type of transaction before from this device), looking at many different relationships.

How these different factors are weighed is determined by using a training algorithm on a large dataset of historical transactions and the “truth data”, i.e., these types of models are inherently “data driven.” This allows models to “discover” non-trivial relationships that are not easy to capture in rules, and to present the best estimate of the likelihood that this is an illegitimate transaction.

The output from these models is a number which provides an estimate of the likelihood that this authentication attempt is *illegitimate.* This admits a rank ordering of the authentication transactions, allowing for different actions to be taken and for prioritization within those actions. In particular, this allows for the “silent authentication” of transactions without impacting the cardholder based upon the behavior patterns in the data that show a low likelihood of illegitimacy.

Non-linear numerical modeling using feed-forward neural networks

Amongst the many available numerical modeling approaches, feed-forward neural networks (FFNN) provide the ideal combination of performance, flexibility, and feasibility.

Feed-forward neural networks are extremely flexible, in that they require no structural or distributional assumptions on the input-feature space. They exhibit state-of-the-art performance on even the most non-linear data, as they are universal function approximators. Moreover, regardless of the size or complexity of the data, they train in linear time, and score in constant time, making them very practical for even extremely large datasets.

Neural network structure

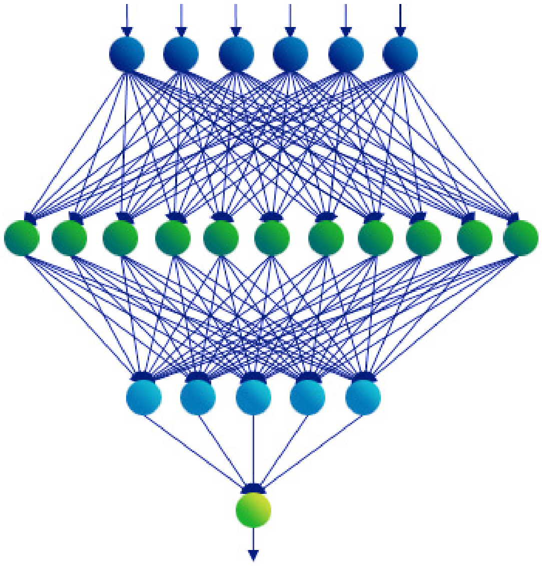
An FFNN is essentially a directed acyclic non-linear signal-flow graph, whose input is a numeric representation of the transaction as captured by the techniques mentioned above, and whose output, in the present context, is interpreted as an ordinal measure of the probability that the authentication attempt is fraudulent (the score).

More descriptively, FFNNs can be thought of as being composed of a sequence of "layers", each of which is composed of a set of "neurons" (see Figure 2). The input authentication attempt is presented to the first (input) layer, where it begins its propagation through the network. This propagation continues through internal layers ("hidden layers"), and finally to the output layer. Each layer performs a non-linear transformation on its input and passes the result onto the subsequent layer. Each layer can have an arbitrary number of neurons, but, in the present context, the final (output) layer has a single neuron (which produces the score).

The expressive power of FFNNs lies in these sequential non-linear transformations, which collectively enable the FFNN to model any function of its input.

Figure 2.

An example Feed Forward Neural Network (FFNN)



Section 3

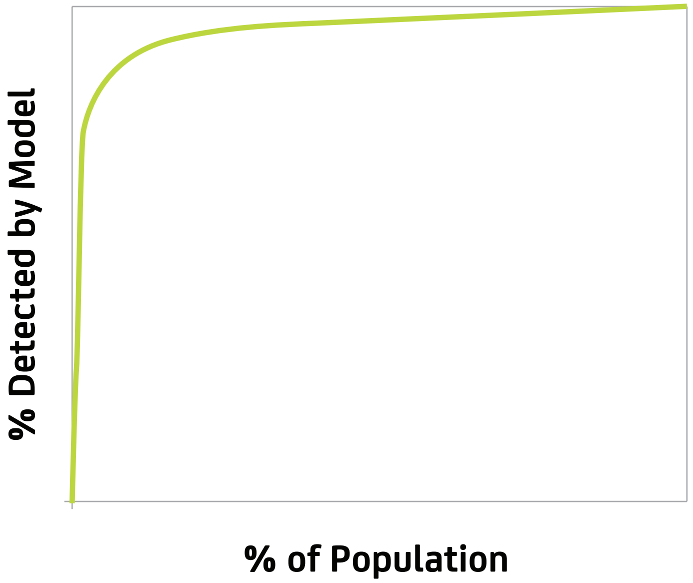
Advantages of Advanced Models

Model performance

CA Regional Models allow denial or increased authentication on a majority of the fraudulent transactions while only impacting a small portion of the legitimate transactions. The general performance is shown in Figure 3. The model maximizes fraud detection while minimizing the impact on the customers. Note that the graph does not display the full curve, instead focusing on the operational area of the curve.

Figure 3.

The fraud detection of the model as a function of the percentage of all transactions flagged by the model. Note that the graph only covers a portion of the population, focusing on the operational area of the curve.



Models scores and rules

Rules are very good at targeting precise, well-known indicators of fraud. They are quick to implement, and easy to understand. However, they are not data driven, and are therefore limited by the knowledge of the rule writer as to the possible signals of fraud. Rules cannot capture complex behaviors easily, and do not readily allow multiple risks to be combined into a single decision. Finally, they cannot rank-order the transactions to allow decline, secondary authentication, and case volumes to be adjusted.

Models capture complex patterns by utilizing sophisticated variables. The variables are based upon the current transaction as well as the pivot distillates (key information from past transactions on pivotal identifiers in transactions, which have been distilled down). Using both non-linear as well as linear variables, and established training techniques, models allow for the weighing of different factors using a data driven approach, and produce a rank ordering of the transactions based upon likelihood of fraud. However, models do not take action by themselves; rules are an essential complement to models.

Rules and models together

Given the different strengths of models and rules, the best approach is to use them together. First, utilize a strong model to separate fraud from non-fraud, and rank-order the transactions using a score. Second, write rules that utilize this score in a few ways: (i) high scores indicate a strong likelihood of fraud, and should be used for taking action, adjusting the score threshold to achieve the volumes and richness of fraud desired by the institution, and (ii) lower scores can be used in conjunction with flash-fraud or other rules, filtering out those with a strong likelihood of non-fraud and allowing the rules to operate in a richer pool of data. Finally, there will be policy rules, which are independent of likelihood of fraud, which the institution implements—perhaps requiring secondary authentication for new devices regardless of the likelihood of fraud.

Section 4

Conclusion

The use of behavior-based authentication to determine which transactions should be impacted by authentication or denial is critical for reducing customer impact (i.e., friction) while creating better assurance that the transaction is legitimate. Rules are an important component when providing this risk- and behavior-based authentication. However, they have a number of limitations. When sophisticated behavior-based models are added, and guide the application of risk-based rules, the impact upon illegitimate attempts can be greatly increased while the impact on legitimate customers is decreased, providing a better experience for the cardholder and loss reduction for the issuer.

Section 5

About the Authors

Paul Dulany has been in the Advanced Analytics and Data Science area for 14 years. He joined CA Technologies in 2013, and led the development of the analytical modeling infrastructure and the first model produced by the CA Data Science team. Prior to joining CA Technologies, he was at the SAS Institute for over 8 years, where he was on the team that developed the first models for the SAS Enterprise Fraud Management solution, as well as leading the development of the first debit card models and developing many new techniques. Prior to SAS, Paul was at HNC and Fair Isaac for over 5 years, as a Scientist and later as the manager of the Fraud Predictor modeling team, developing a number of Falcon payment card models as well as working in other areas. Paul holds patents from his time at HNC and SAS, and has a Ph.D. in Theoretical Physics.

Hongrui Gong has extensive experience in the area of Advanced Analytics and Data Science. He joined CA Technologies in April 2013 and played a key role in the efforts of building a modeling infrastructure and developing models for 3D secure products. Prior to joining CA, he worked for more than 15 years with prominent analytic companies (SAS, FICO, and HNC) to develop models for products such as payment card fraud detection, insurance fraud detection, tax under-filers identification for federal and state government, anti-money laundry, loan loss forecast, brokerage margin landing risk management, and credit risk rating for public and private companies. Hongrui has a PhD in Computational Fluid Dynamics and spent 4 years in Los Alamos National Laboratory focusing on the research of theoretical modeling and computer simulations of turbulent fluid flow. He holds a number of patents from his prior work.

Kannan Shah has been in the Advanced Analytics and Data Science industry for 6 years. He joined CA Technologies in 2013, and contributed to the development of the analytical modeling infrastructure and the first model produced by the CA Data Science team. Prior to joining CA Technologies, he was Senior Staff Scientist at the SAS Institute, where he developed statistical models and techniques, and provided client support, for the SAS Enterprise Fraud Management solution. He has contributed to the development of fraud-detection models for payment cards and ACH- and wire-transfers, deployed in the US, the UK, Mexico, and the Asia-Pacific region. Kannan holds a number of patents from his time at SAS. Kannan has a MS degree in Electrical Engineering from Drexel University in Philadelphia. His areas of focus during his academic studies included detection and estimation, stochastic signal processing, machine intelligence, statistical pattern recognition, neural networks, information theory, higher-order spectral analysis, and algorithm design and complexity.

ca technologies

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

[1] In regions where there has been significant cardholder education to look for 3D-Secure indicators, it may be reassuring to the cardholder to pop up a window stating that this transaction is protected by 3D-Secure.

[2] The term “truth data” refers to transaction and card level information to identify the transactions that the authentication process should stop.