DEPTH. FOCUS. SERVICE.

MERCATOR ADVISORY GROUP

AUTHENTICATION, INTELLIGENCE, AND THE CONSUMER JOURNEY:

A MULTILAYERED APPROACH TO REDUCE DIGITAL FRAUD

Mercator Advisory Group Research Brief Sponsored by Mastercard

mastercard

December 2019

Contents

201 Boston Post Road West, Suite 301 | Marlborough, MA 01752
phone: 1-781-419-1700 | email: info@mercatoradvisorygroup.com
www.mercatoradvisorygroup.com

Executive Overview

This Mercator Advisory Group research brief outlines a new strategy for managing payments risk that is multilayered, risk-based, and holistic, a strategy that Mastercard calls "connected intelligence." We argue that rather than rely solely on information available at the time of a payment, financial institutions and merchants do better by collecting data in advance, taking advantage of new capabilities in biometrics and data analytics. This approach can reduce by 90% the number of "false positives," or targeting of legitimate customers for further authentication, dramatically reducing shopping cart abandonment and enabling merchants and card issuers to focus on the biggest threats. This approach will also help combat the runaway epidemic of "friendly fraud" — the improper use of the dispute process by consumers — which various sources have found may be the source of anywhere from 25% to-80% of all chargebacks, arguably the bigger problem.[i]

Financial institutions and their customers are under attack by criminals who have harvested literally billions of consumer credentials, which are then used for synthetic fraud, account takeovers, and payment fraud. While security is a top concern for every business, many executives remain unaware of the potential of new fraud technology. And merchants are caught between the desire to make the payments experience as seamless as possible and protecting themselves from criminals as well as from customers who are abusing the dispute process.

This paper addresses two main topics. First is non-payment authentication, or the validation of identity before the customer ever gets to a shopping cart page. Second is payment authentication, or the combining of the data collected beforehand with the data collected at the time of purchase. We describe the new EMVCo standard, 3-D Secure 2.0, and explain how it embodies this strategy by vastly increasing the amount and types of data available to score an authorization request. We also explain how this data is created through a combination of behavioral analytics, passive biometrics, and active biometrics.

Instead of a binary (yes/no) authentication decision, it is possible to work with degrees of certainty. Based on the size and context of a purchase, a confidence level of 85% or less may be perfectly acceptable. In fact, this is the reasoning many merchants apply as they prioritize customer satisfaction over fraud prevention. However, these decisions can be made with even greater precision. Friendly fraud is something that can also be addressed through better data analysis, by making it easier for the merchant to prove that a customer did in fact make a purchase. For example, a merchant can determine that a customer was exhibiting normal behaviors prior to a purchase and was previously authenticated through the customer's mobile device.

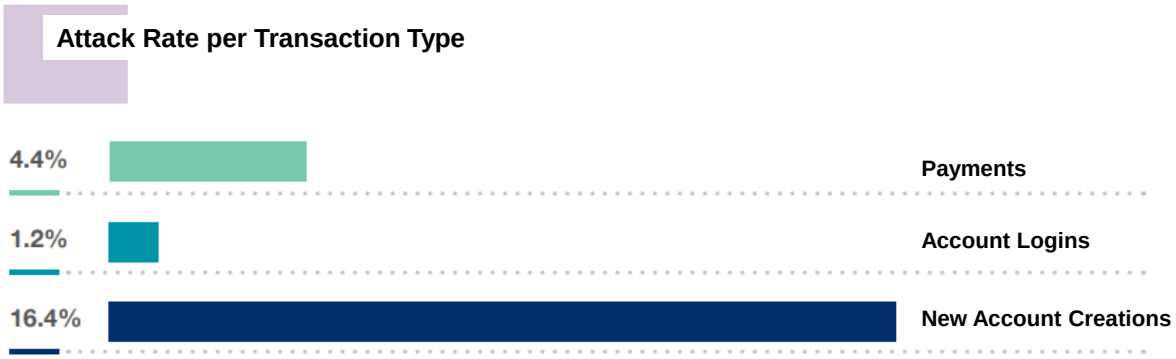
We briefly touch on the concept of self-sovereign identity (SSI), a new approach to authentication based on blockchain and smart contract technology that allows a customer to reveal only that information necessary to authorize a single transaction, often without revealing the actual data itself. SSI and other digital identity technologies, such as FIDO, will enhance the power of EMV 3-D Secure, EMV Secure Remote Commerce (SRC), and other holistic security strategies by providing highly secure, reliable data to work with. The degree of certainty will increase without requiring any additional work and will better protect personal privacy.

By the end of this paper, you will be equipped with a working knowledge of the latest authentication practices for use in charting your own business's security strategy.

The High Levels of Fraud in Digital Commerce

As card issuers, networks, and merchants have made the shift to EMV chip card authentication at the physical point of sale, fraud has migrated to the online channel, where there is no clear equivalent, at least not one with a similar mandate. A recent study by Lexis/Nexis Risk Solutions found that attack rates are particularly high for account creation and for payments, the subjects of this paper, while some progress has been made in protecting account logins.[ii]

Figure 1. Attack rates continue to be high for payments and account creation.



Attack rate is based on percentage of transactions identified as high-risk and classified as attacks, by use case. Events identified as attacks are typically blocked or rejected automatically and in real time depending on individual customer use cases.

Source: Lexis/Nexis Risk Solutions, 2019

The practical result of the migration of fraud to the online channel has been a shift in liability to the merchant, who often does not have a good way to dispute chargebacks by cardholders. Some of this fraud is what is termed in the industry "friendly fraud," which can take several forms:

- The cardholder disputes a purchase that the cardholder did in fact make, without making a good faith effort to work it out with the merchant.

- The cardholder disputes a purchase because the cardholder does not recognize the charge on the statement, which can occur when a merchant uses another merchant's account due to a reseller arrangement.

- The cardholder regrets a purchase, and the merchant does not allow refunds (as is often the case for digital goods), so the cardholder seeks to use the dispute process to reverse the charges.

Merchants urgently need to have a more effective strategy for addressing disputes and authenticating customers so as to make it more difficult for customers to dispute legitimate transactions. One way to do this is to consider an authentication strategy that encompasses both payment and non-payment authentication so that consumers are verified and fraud mitigated even before a transaction begins. In the remainder of this white paper, we discuss some of the payment and non-payment authentication strategies available and how advances in machine learning and AI offer a path to a secure and seamless experience for a consumer. With various reports suggesting that up to 80% of chargebacks may actually be friendly fraud, this is a serious issue. There are companies, like Ethoca, a Mastercard company, that have purpose-built solutions for tackling friendly fraud.

Global Travel Company Achieves 100% Success in Blocking Fraud

According to Mastercard, a global travel company was being hit with large-scale fraudulent transactions as well as seeing accounts being created for fraud. With thousands of sessions per day, the company needed a solution that could scale without inconveniencing valid users.

Using behavioral biometrics intelligence, the travel company was able to verify 99% of legitimate users in real time—adding friction on suspicious traffic only. They were also able to discern which accounts were created fraudulently before they could generate losses.

The results were over 400,000 suspected fraud events blocked per day, 99% of legitimate users authenticated, and 100% of attacks blocked.

Non-Payment Authentication

The category called "non-payment authentication" includes strategies to identify potential fraud before it occurs in the form of a purchase. These strategies include behavioral analytics (noting behavior inconsistent with past patterns or indicative of fraud risk), passive biometrics (usage patterns that may indicate fraud), and active biometrics (authentication challenges) to aid in the authentication process.

Biometrics

Non-payment authentication requires a combination of passive biometrics (closely associated with behavioral analytics) and active biometrics (challenges to the user). To avoid challenging the cardholder every time a transaction needs to be authorized, the cardholder's interaction with the browser or mobile access device can be monitored as the person goes about daily activities. Metrics monitored include things like typing speed and location data. Behavioral analytics to identify a device user's typical patterns of behavior can be added to establish

confidence that the device has not been compromised and is not controlled by a new (possibly fraudulent) user. Passive biometrics use cases may include simple account logins to social media accounts, or merchant accounts where a transaction need not occur. Behavioral biometric technology, which enables early risk monitoring at the edge of the network when visitors first enter a website, is already deployed in a range of fraud protection platforms, including security platforms offered to merchants and issuers by the payment networks. Industry leaders like NuData, a Mastercard company, use machine learning to construct models of standard behavior for each cardholder based on biometric data; deviation from these models may be an early indicator of account takeover. Conversely, when the models conform to the actual behavior but fraud is claimed, they can be used to buttress counterclaims that the buyer actually did authorize the purchase.

Use of active biometrics, such as fingerprint scanners, facial recognition, and voice recognition, when built into the operating system to provide access to the device and secure applications, can further reinforce confidence. As more and more devices have equipment such as webcams, video chat, and microphones, capturing biometric data is becoming much easier. Financial institutions should use these technologies instead of relying only on user IDs, passwords, and challenge questions. (Challenge questions can easily be solved through a simple Facebook or Google search or by consulting publicly available databases. User's birthplace or mother's maiden name are examples of common challenge questions whose answers can easily be found that way.)

Active biometrics is much more relatable in our everyday lives – from fingerprint scanning to make a purchase via a mobile device, to newer, more exciting use cases aimed to simplify the customer experience such as facial recognition to check in or board a flight. As with passive biometrics, machine learning and artificial intelligence are integral to the construction of a unique profile that can be checked against later samples (say, of a fingerprint, face, or speech).

FIDO

FIDO,[iii] short for "Fast ID Online," is a cross-industry initiative with members from all the major payment networks, many of the large security platform providers, several international, regional, and smaller banks, and platform suppliers such as Google, Facebook, Microsoft, and Verizon, as well as major investment firms.[iv] FIDO works to establish standards for authentication that allow interoperability across industries — from the issuer to the network to the device manufacturer to the merchant. A primary goal is the gradual replacement of user ID and passwords with biometrics securely stored on the buyer's device as the new means of authentication. The next step is to extend the local device's biometric capabilities to any remote application approved by the device owner. The extension of biometric capabilities is accomplished by using an authentication protocol based on public-key cryptography. This enables the user to provide proof of a biometric match when challenged by any number of organizations without revealing any personal information. Each organization utilizes a unique key pair that is not shared with anyone else. As a result, no organization needs to create a huge database of user IDs and passwords that attracts criminals and the user has no need to memorize lots of passwords.

Payments Authentication

This section discusses strategies that take advantage of new technologies for authenticating the identity of purchasers as they make transactions. As in non-payment authentication, behavioral analytics and passive biometrics are an important first line of defense, to create data that can inform the decision to approve the purchase request.

A second line of defense consists of technologies for securing e-commerce transactions — EMV 3-D Secure 2.0 and Risk-Based Authentication (RBA) — both described below. A third and final line of defense is active biometrics, such as fingerprint or facial recognition, which can be part of the second line of defense or operate on the device level independently.

EMVCo 3-D Secure

EMVCo's technology push to secure e-commerce started with 3-D Secure 1.0 in 2011. The messaging protocol relied on two-factor authentication but was unpopular with merchants because its unintuitive enrollment procedure led to elevated rates of shopping cart abandonment. Subsequent updates improved the process to be more transparent, but by then many merchants had ceased using it. EMVCo is trying again with 3-D Secure 2.0, which makes substantial workflow improvements and is entering a market that is more receptive than before in light of increased incidence of fraud.

EMV 3-D Secure 2.0 (3DS2) is a major redesign of 3-D Secure that uses auto-enrollment to increase cardholder participation. Most important, 3DS2 will greatly reduce shopping cart abandonment because it reduces how frequently a cardholder needs to be actively authenticated (i.e., bank login, challenge questions, or biometrics). It does this by using a risk-based process to shift the authentication for many transactions to the issuer. The new tools outlined above, along with transaction history and other factors, ensure that only high-risk transactions need to be actively authenticated. These improvements should overcome the concerns that merchants had with the first version of EMV 3-D Secure.

When a card issuer turns on 3DS2, the protocol automatically enrolls all of the cardholders that participate in that issuer's designated card ranges. Should a cardholder be challenged during an e-commerce transaction, that cardholder will be able to utilize either the secure active biometric or a one-time passcode utilized by the issuing bank. But avoiding a challenge would be the best approach. So, without a doubt, the most important improvement is the additional data that merchants will send the issuing bank with every authorization request. The additional data will reduce the percentage of transactions requiring active authentication to about 10%, according to tests by the EMV members. As before, machine learning and artificial intelligence are key to making the best use of all the additional data.

3DS2 provides the merchant with a way to transmit data extracted from consumer access devices, which includes mobile and desktop computers. The data is then combined with information related to the merchant account and sent to the issuer. The specification mandates 40 data elements but allows up to 150 different data elements to help the issuer better evaluate the transaction. The additional data is sent using the Access Control Server, or ACS, a service operated by the card issuer to handle 3DS2 authentication requests, while the traditional authorization request is sent as usual (see *Figure 2*). Merchants that adopt 3DS2 are protected from liability for fraud just as they are when they adopt EMV and accept physical EMV chip cards.

However, correct implementation is important to avoid problems later on. Merchants need to ensure that they:

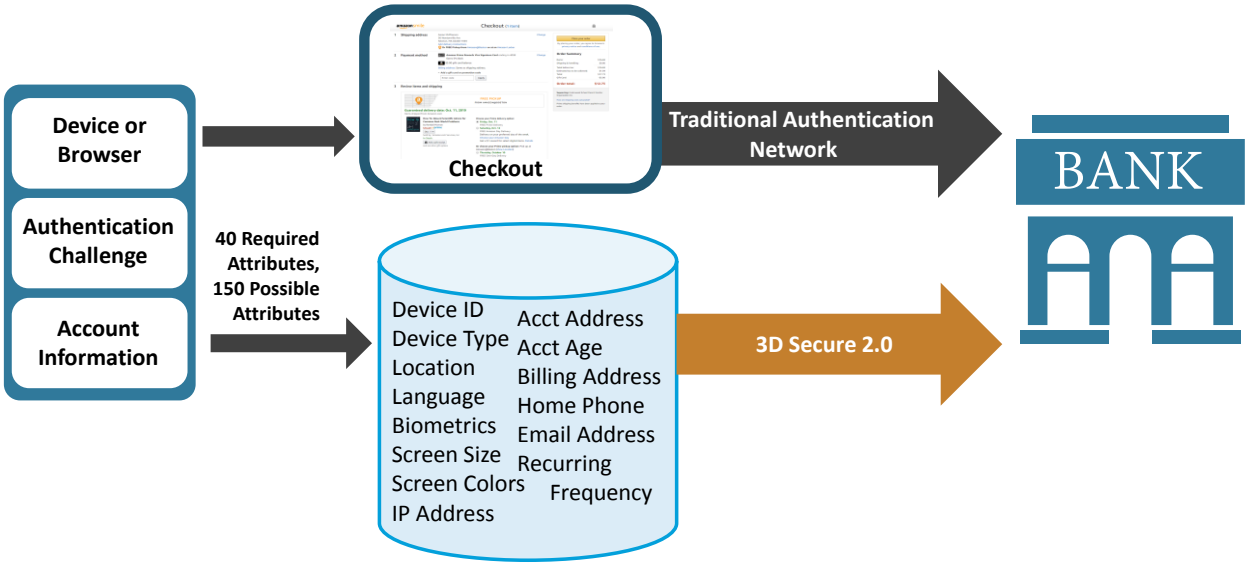
- Have access to data elements like the account holder's device ID, payment account number, and address to send with the authorization request.
- Are monitoring the data that is being collected for 3DS2 to ensure that they are following the correct format as given in the EMVCo specification.
- Include account holder authentication value and security-level indicator in the payment authorization message. Payment gateways and acquirers can help with this.

Access Control Server Response Time Emerges as Top Issue for EMV 3-D Secure 2.0

The best security is of no use if it cannot be used reliably and efficiently. EMV 3-D Secure 2.0 (3DS2) relies in part on an Access Control Server (ACS) run by the card issuer to respond to authentication requests.

During testing of Mastercard's implementation of 3DS2, called Mastercard Identity Check, endpoint access was found to be early adopters' number one issue (indicated by 72%). Issuers need to check their firewall settings to ensure that they are not causing processing and time-out errors.

Figure 2: Under EMV 3-D Secure 2.0, issuers receive a minimum of 40 additional data points for risk analysis.



Sources: EMVCo and Mercator Advisory Group

Risk-Based Authentication

The general idea behind risk-based authentication (RBA) is that the level of authentication should be proportional to the risk. This strategy is built into 3DS2, as we have seen, to reduce legitimate customers' inconvenience and shopping cart abandonment. Risk is assessed using all the techniques discussed above as well as factors specific to the payment (dollar amount, buyer location, past history of disputes, etc.).

An option for issuers is to utilize the payment network's stand-in service such as Mastercard's Smart Authentication solution, which generates a risk score and will issue the challenge if required. It is likely the network can generate a more comprehensive risk score than the institution could because the network has access to a wider range of transactions, merchants, and merchant categories, which can be used to enhance accuracy. In this scenario, the card issuer identifies the risk score that represents an unacceptable level of risk.

These risk scores use machine learning and artificial intelligence to relate incidences of fraud to the data captured before, during, and after the transaction and to assess the strength of the correlation. Weaker correlations produce scores with lower confidence, which can fall below the threshold for further action. Stronger correlations produce higher scores, which can trigger further authentication challenges. The key is to step up the challenges in accordance with risk so that far fewer transactions require challenges.

Self-Sovereign Identity (SSI)

The idea of self-sovereign identity (SSI) is that individuals should be able to control the use of their own data and have a credential that can be used in a variety of contexts. Key players including IBM, Microsoft, and Mastercard have indicated their support for SSI or have established policies that embrace this new approach to identity management. SSI enables an authenticated customer to verify only the specific information requested by an organization for the purpose of enrollment. For example, the customer can have the state verify she is over 21 and have her bank verify that she earns more than $100,000 annually. This is done without releasing the person's actual age or income by means of a technology called "zero-knowledge proof."[v]

At the same time, this solution logs all of the data the person has released and to whom while also enabling fees to be applied by the authenticator to the validator. Financial institutions that agree to validate claims can receive a fee for this service. Self-sovereign identity fits very well in the framework discussed in this paper and can be an input for 3DS2, FIDO, and the overall integrated authentication approach.

Going forward, we expect to see SSI and other federated identity schemes extending and enhancing the end-to-end security offered by existing schemes.

Conclusions

The detection and prevention of fraud has changed dramatically with the introduction of large-scale data analytics and machine learning that can access many more data points than were previously available. A holistic view of payments, or *connected intelligence,* extending back to the customer's daily activity, behavior patterns, and technology usage and forward to the purchase and authorization, can dramatically reduce the incidence of fraud. It is no longer enough to score a transaction based on the information available at the time.

Customers have more choices than ever before as to where and how to shop, and merchants pay a heavy penalty for authentication processes that require customer involvement. By collecting data before the payment, through behavioral biometrics, active biometrics, and pattern recognition, merchants and financial institutions can work together to do most of the work in advance so that the customer is authenticated *before* making a purchase. Active authentication is only required in truly exceptional cases, 10% of the time or less. Strategies that work across channels can create even more data to reduce the need for active authentication. Self-sovereign identity is a developing technology that will reduce the need for so much data collection by allowing customers to prove their identity up front, without revealing as much personal data.

With data an integral part of every digital experience, it is critical that the collectors of this data take responsibility to ensure its proper use. Whether working with others in the industry, with networks, or with new entrants, data privacy and adherence to best practices are imperative. The right partnerships can ensure that data and the insights gained from the data are used to drive commerce forward for good. A good example of data responsibility is Mastercard's Global Data Responsibility Imperative, six principles that guide Mastercard's own practices.[vi]

Mercator Advisory Group strongly recommends that financial institutions implement an authentication strategy that leverages the full spectrum of active and passive biometrics as well as big data, machine learning, and behavioral analytics. This strategy should follow a risk-based model, layering security so as to reach the ideal balance between convenience and risk. Fortunately, there is plenty of support available from device manufacturers, payment networks, payment processors, and specialty vendors.

Endnotes

[i] See, for example: https://www.chargebackgurus.com/blog/what-is-a-chargeback, and https://chargebacks911.com/chargeback-stats/, accessed 11/6/2019.

[ii] https://www.threatmetrix.com/info/cybercrime-report-january-june-2019/, accessed 10/9/2019

[iii] https://fidoalliance.org/what-is-fido/

[iv] https://fidoalliance.org/members/, accessed 8/7/2019

[v] https://towardsdatascience.com/what-are-zero-knowledge-proofs-7ef6aab955fc?gi=28d3fbf3baae, accessed 8/8/2019

[vi] See https://www.mastercard.us/en-us/about-mastercard/corp-responsibility/data-responsibility.html

About Mercator Advisory Group

Mercator Advisory Group is the leading independent research and advisory services firm exclusively focused on the payments and banking industries. We deliver pragmatic and timely research and advice designed to help our clients uncover the most lucrative opportunities to maximize revenue growth and contain costs. Our clients range from the world's largest payment issuers, acquirers, processors, merchants, and associations to leading technology providers and investors. ***Advisory services*** include *Credit, Debit and Alternative Products, Prepaid, Merchant Services, Commercial and Enterprise Payments, Emerging Technologies,* and *Global Payments* practices, which provide research documents and advice. ***Primary Data services*** include the *North American PaymentsInsights series*, which report and analyze data collected in our bi-annual consumer surveys, as well as the annual *Small Business PaymentsInsights* and *Buyer PaymentsInsights series.* ***Consulting services*** enable clients to gain actionable insights, implement more effective strategies, and accelerate go-to-market plans; offerings include tailored project-based expertise, customized primary research, go-to-market collateral, market sizing, competitive intelligence, and payments industry training. Mercator Advisory Group is also the publisher of the online payments and banking news and information portal PaymentsJournal.com. Visit www.mercatoradvisorygroup.com.

About Mastercard

Mastercard (NYSE: MA), www.mastercard.com, is a technology company in the global payments industry. Our global payments processing network connects consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard products and solutions make everyday commerce activities – such as shopping, traveling, running a business and managing finances – easier, more secure and more efficient for everyone.