Introduction

The numbers are in – and they're not pretty. Even before the unprecedented interference of a global pandemic hit our shores, merchant losses to eCommerce fraud were projected to grow to $6.4 billion by this year. Meanwhile, losses due to false declines were projected to reach $443 billion – nearly 70 x more than losses from fraud itself. In fact, **62% of online merchants saw an increase in their decline rates as far back as 2019.**[1]

Because merchants often overcompensate by declining any transaction they deem suspicious of fraud, they actively harm both their bottom line and the consumer experience. Balancing revenue and fraud prevention without negatively affecting customers is vital if merchants wish to stay in the game.

In this eBook, let us set the 2021 eCommerce scene; introduce to you the various players in online transactions; examine the ways in which false declines can be costly; and, most importantly, detail how your business can reduce them.

[1] Aite Group, The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention, Shirley Inscoe, July 10, 2019

THE GROWTH OF ECOMMERCE

Since the beginning of 2020, there has been explosive growth in eCommerce, especially when the shelter-in-place mandate was established in the US (+100%, Month, DD, 2020). We saw similar trends in Europe (+30%, Month, DD, 2020) as well as Asia (+50%, Month, DD, 2020), according to the COVID-19 Commerce Insight dashboard. In fact, according to data released from IBM's U.S. Retail Index[2] , the pandemic has accelerated the shift away from physical stores to digital shopping by an estimated five years.

THE INCREASE IN CARD-NOT-PRESENT FRAUD

It's simple. Because it's an easy and convenient payment method for online shopping, there has been a natural surge in contactless card use. Unfortunately, with this increase in digital card-not-present (CNP) transactions, we have seen a corresponding rise in CNP fraud claims. In fact, again, even before COVID-19 was declared a pandemic, the Aite Group report projected a 16.4% increase in U.S. CNP fraud this past year alone.[3]

THE CHALLENGES IN FIGHTING FRAUD

While the growth in eCommerce is no doubt beneficial for consumers and merchants alike, the challenges are obvious. The rise in online purchasing behavior creates a growing opportunity for bad actors and cybercriminals to defraud digital businesses of millions of dollars a year.[4] In this "new normal," with increased online traffic and transactions, comes a greater focus on approving the good customers, known or unknown. However, when businesses implement or tighten fraud detection measures, some good customers are falsely identified as fraudulent. Reducing these false declines (falsely identifying good customers as fraudulent) in fraud models is key to saving and growing revenue in a digital-heavy economy.

Fraud Prevention Obstacles

This rise in fraud sophistication has driven merchants to put measures in place to minimize fraud losses, but in doing so, they face the challenge of rising false declines.

[2] TechCrunch.com, Covid19 Pandemic Accelerated Shift to eCommerce by 5 years New Report Says, Sarah Perez, August 25, 2020
[3] Aite Group, The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention, Shirley Inscoe, July 10, 2019
[4] Forbes·com· How E-Commerce's Explosive Growth is Attracting Fraud· Louis Columbus· May 18, 2020

The Players

THE FRAUDSTER: THE CLEVER CRIMINAL

Fraudsters erode revenue by finding weak paths. By creating a synthetic identity or tweaking electronic data to steal an identity, a fraudster gains dishonest advantage over both individuals (the consumers) and businesses (the merchants).

THE FRAUDSTER: THE CLEVER CRIMINAL

Consumers demand a frictionless, secure experience or they will take their business elsewhere. Should a consumer be impeded by too many verification requirements to prove their identity; or worse, should a transaction be declined, their loyalty will be tested.

THE MERCHANT: THE LIABLE PARTY

Each and every online merchant in the game balances the risk of transaction with the revenue impact to a customer's lifetime value. With any fraud detection solution that a merchant puts in place, they must ask themselves: Will this prevent fraud while also delivering a superior experience to the end consumer?

False Decline Options

Because the cost of false declines is so great, many merchants implement systems to evaluate whether declined transactions are truly fraudulent. There are several methods by which this is done:

- Call center monitoring
- Manual reviews
- A/B testing

These can be done in-house, without the use of third-party data. However, using third-party data can limit the risk and cost of evaluating false declines.

{Please see Appendix for details}

THE PROBLEM: REDUCING FALSE DECLINES TO RETAIN GOOD CUSTOMERS

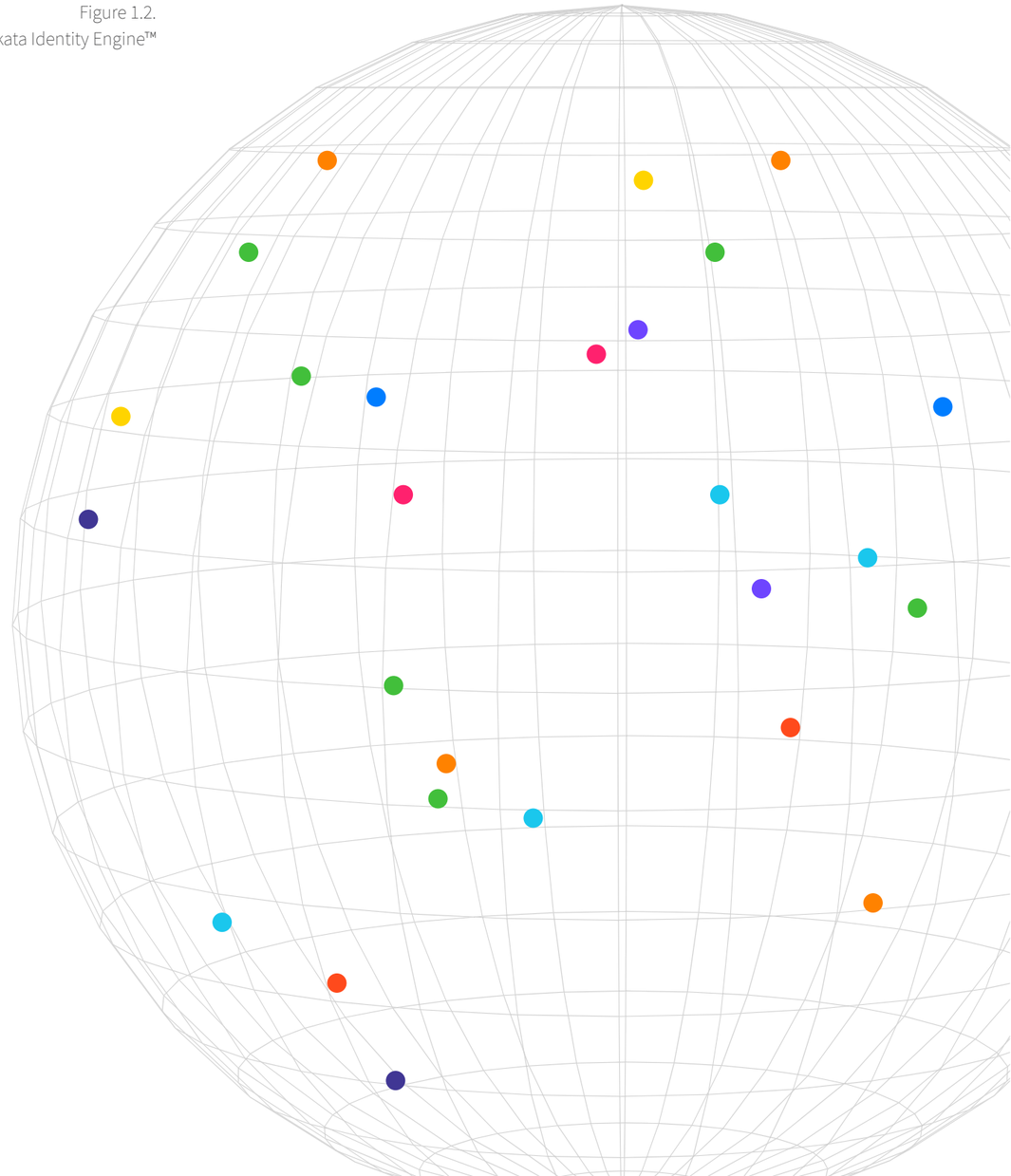
It's a delicate balancing act for online merchants; the need to reduce friction for customers while ensuring they are authenticating payments appropriately. All this while preventing loss from fraudsters. While it appears to be a complicated, multi-faceted problem, there is a solution.

THE SOLUTION: STREAMLINE THE PAYMENT PROCESS

As an identity verification solution provider, Ekata has worked with many merchants streamline the payment process. While definitions may vary across industry, there are three points in the payment process that Ekata has identified where a transaction can be rejected: pre-authorization, authorization and post-authorization.

Proactive pre-authorization screening for merchants allows them to capture fraudulent transactions early on and help move good customers through the workflow. In the event that uncertainty remains after a transaction has been authorized (post-authorization), a manual review tool can be used to further assess the riskiness of the customer.

Figure 1.2.
The Ekata Identity Engine™



A Machine Learning Approach

Ekata products are powered by the Ekata Identity Engine (EIE) which uses complex machine learning algorithms across consumer attributes to derive unique data links and features from billions of real-time transactions within our customer network and globally sourced data.

FUELED BY PREDICTIVE POWER

To score the predictions of machine learning algorithms, we use what is called a confusion – or error - matrix. Its output is a summary of predicted results that describe the performance of a classification model where a set of data could be labeled as true or false.

		Actual Values: Positive	Actual Values: Negative
Predictive Values	Positive	True Positive	False Positive
Predictive Values	Negative	False Negative	True Negative

The Ekata risk scores predict the validity of the customer - specifically, where the actual values are observed fraud.

Some merchants have more sophisticated models than others. For those who may not have a risk assessment model in place, they will initially see a mix of good transactions and bad transactions. From there, they can use metadata collected from customers to build a fraud model. In the simplest terms, the best model balances false positives, false negatives, true positives, and true negatives based on the risk tolerance of the use case.

For merchants who already have a risk assessment model in production, the reality is different. It is possible that the merchants may already have rules to block a set of users. In such a case, actual values can be determined through manual review or a control group.

FALSE POSITIVES AND NEGATIVES

Within the confusion matrix, the Ekata model could categorize the customers into the quadrants.

		Actual Values: Positive (Fraud)	Actual Values: Negative (Not Fraud)
Predictive Values	Positive (Fraud)	Fraudsters	Good Customers labeled as Fraudsters
Predictive Values	Negative (Not Fraud)	Fraudsters Perceived as Good Customers	Good Customers

For fraudsters who are perceived as good customers, they will likely be captured through the payment process which eventually could result in a transaction decline or a manual review of their validity. For good customers that have been categorized as bad, the outlook and outcome can be unknown. Will the customer proactively advise the merchant that they have been declined? Will the customer stay silent and instead pursue a different merchant? Or, will the customer abandon its shopping cart altogether and forego the purchase for the time being?

Implementing Ekata

The approach to capturing fraud and false declines varies from company to company and from industry to industry. By inserting identity verification products into risk assessment models, an additional layer of detection is implemented. Ekata conducts a backward-looking data test to determine what the breakdown of good transactions versus bad transactions would look like if Ekata had been implemented. As anticipated, outcomes for accepted transactions is straight forward, whether it is fraud or not. Outcomes for rejected transactions are less clear, but can be seen through an Ekata lens.

RISK SCORE

As part of the Ekata data responses, proprietary risk scores are highly predictive signals that are designed to help differentiate good customers from bad customers.

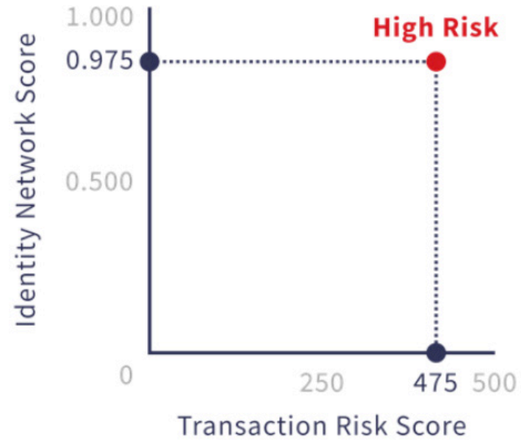
Identity Network Score:
Assesses only how identity information is being used in digital interactions

Transaction Risk Score:
Validates who the customer is and how their information is being used in a digital interaction

The two scores independently predict a risk level based on the input from the transactions. The Identity Network Score spans a spectrum from 0 to 1 where 1 denotes high risk. Similarly, the Transaction Risk Score spans a spectrum from 0 to 500 where 500 denotes high risk.

PROFILING

With the two risk scores, each customer's predicted risk levels could be plotted onto a graph. A customer with an Identity Network Score of 0.975 and a Transaction Risk Score of 475 is deemed to be high risk.

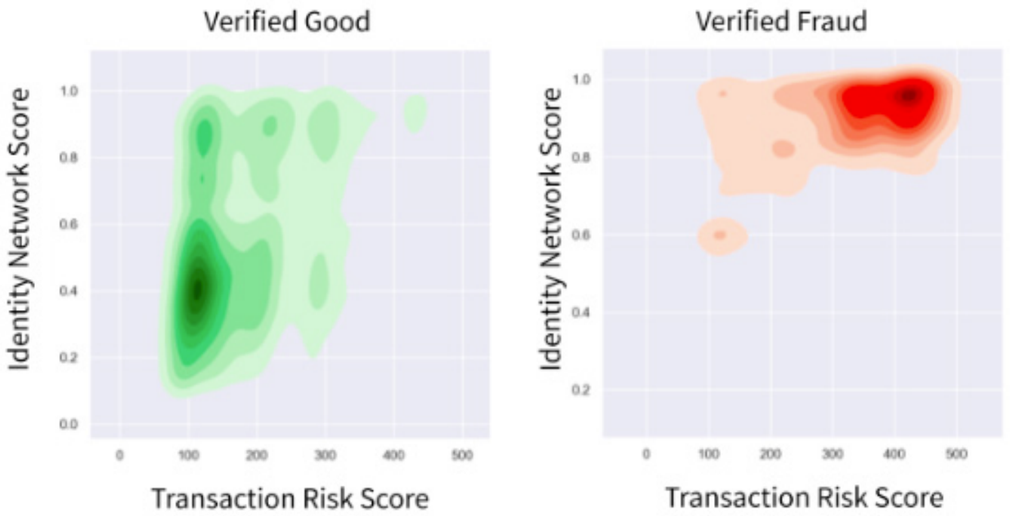


DISTRIBUTION OF CUSTOMERS

Plotting the two risk scores for each customer within a transaction period can help to give us a visual profile of different categories. The green graph represents transactions that are true negative - these transactions were predicted not to be fraud and they were, indeed, not fraud. The red graph represents transactions that are false negative - these transactions were predicted not to be fraud but they turned out to be fraud.

Customers that are verified to be good customers have a greater concentration around an Identity Network Scores of less than 0.6 coupled with Transaction Risk Scores of less than 200.

Customers that are verified to be fraudsters have a greater concentration around an Identity Network Scores of more than 0.8 coupled with Transaction Risk Scores of more



The combination of Transaction Risk Score and Identity Network Score paints a very different picture for good transactions than for bad transactions. Using this information and recognizing that some rejected transactions are good customers, one can make an educated guess on which of those rejected transactions were good customers.

With this set of results, one could also deduce that those rejected transactions in the upper right quadrant are highly likely to be fraudsters - a good indicator that fraudulent transactions are captured properly. Those that fall within the upper left quadrant are indeterminate and signals that more due diligence is required to assess their riskiness. However, those that fall within the bottom left quadrant are likely to be false positives.

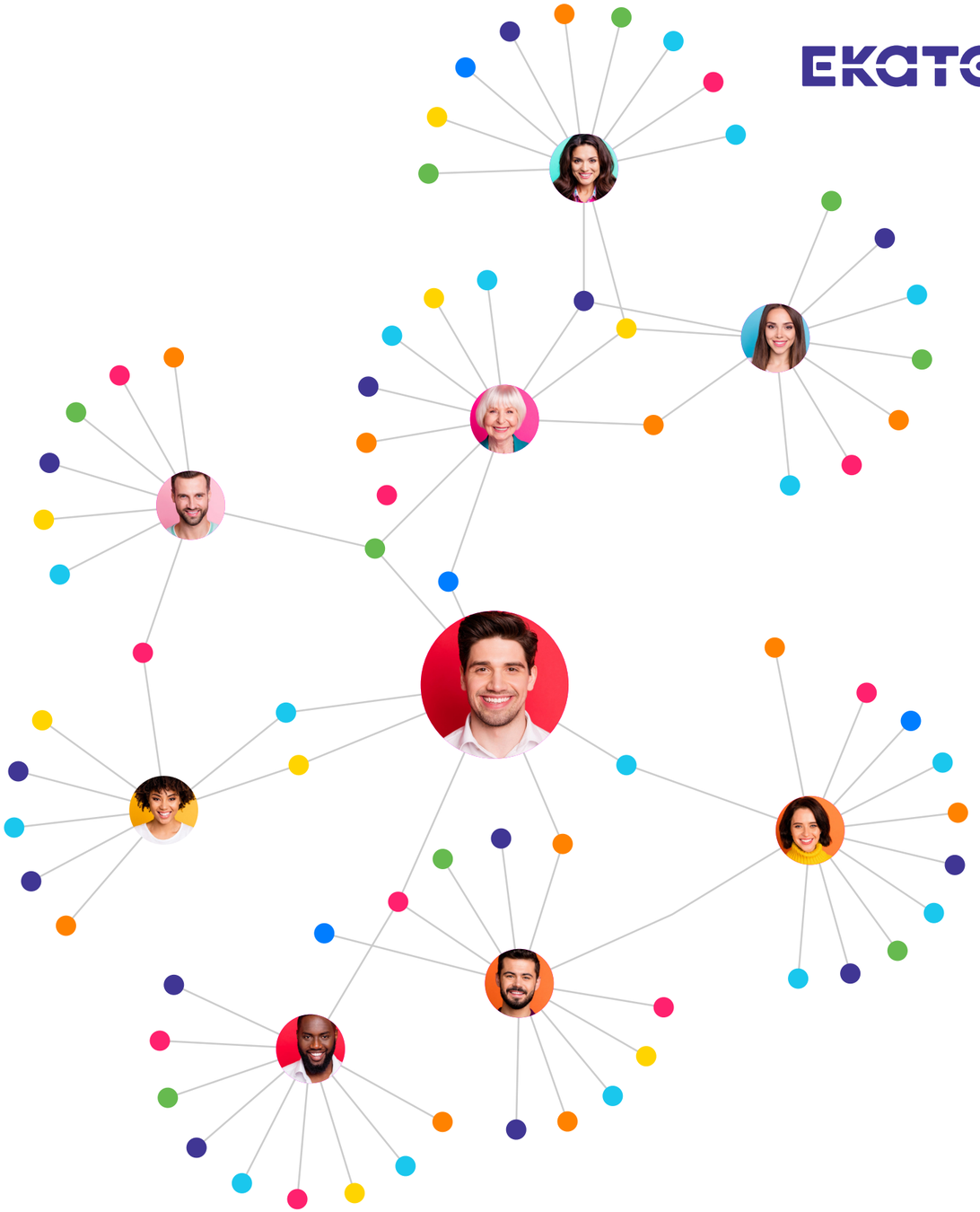
This illustration depicts an Ekata customer test scenario using the methodology of evaluating risk scores to identify false declines. In analyzing its rejected transactions and focusing on the “likely good” transactions, the customer was able to deduce that the bottom left sector of rejected customers accounted for approximately 20% of all rejected transactions. If our customer had implemented an Ekata solution to adjust and update their rules to accept these transactions, they could have seen an increase in monthly revenue by up to $500,000.

In summary, the results of these studies give confidence that the two risk scores play a key role in identifying the uncertainty of rejected transactions. By eliminating the falsely rejected transactions, good customers would encounter less friction and a more positive experience.

Conclusion

It’s simple, really. By identifying false positives and reducing the associated declines, merchants prevent potential revenue loss and, in turn, increase revenue. In choosing to implement an intelligent layer of fraud protection like Ekata, a merchant can proactively set themselves forward to capture fraudulent transactions earlier, allowing good transactions to be processed and, in turn, reducing false declines that are passed through the payment workflow.

To learn more about how Ekata can help your business reduce false declines and minimize the potential revenue loss from customer churn, please contact us for a demo today.



Appendix Table

Appendix: Details on In-House False Positive Detection Methods

	Call Center Monitoring	Post-Mortem Manual Review	A/B Testing
Method	A falsely declined customer contacts the merchant to dispute.	Rejects are sent to manual review; agents determine if the rejection was a false decline.	At random or semi-random, allow a percentage of declined transactions through to determine if they would result in a chargeback.
Resolution	An agent approves customer's transaction; does not result in a chargeback.	An agent determines whether the transaction should have been accepted.	If the order does not end up in a chargeback, then we know it would have been a false decline. If it does end up in a chargeback, then it would have been a correct decline.
Positives	• Clear indication of a false decline problem • Call center cost could be accounted for • Information is easy to collect	• Does not risk additional fraud	• Actual results of good customers vs bad customers
Negatives	• Only select customers will call in • Very few data points, not enough to determine impact	• Manual review agent decision is subjective • Agent resolution may be inconsistent • Labor intensive and costly	• Take on risk • Cost to allow for fraud could be substantial
Recommendations	• Combine method with other solutions • Ensure consistent monitoring and labeling from agents • Ability to link call center logs to false positive claims	• Provide explicit guidance to review agents • Give agents tools such as Ekata Pro Insight	• Select less risky population • Decrease percentage of rejects to the minimum to achieve statistical significance • Select transactions based on low risk scores from Ekata API Solutions

EKATA

WHAT'S NEXT?

Making the Change

About Ekata

Ekata provides global identity verification solutions via enterprise-grade APIs for automated decisioning, and Pro Insight, a SaaS solution for manual review for cross-border businesses to grow revenue by maximizing their predictability of good transactions. Our product suite is powered by the Ekata Identity Engine (EIE), the first and only cross-border identity verification engine of its kind. It uses complex machine learning algorithms across the five core consumer attributes of email, phone, name (person or business), physical address, and IP, to derive unique data links and features from billions of real-timetransactions within our proprietary network and the data we license from a broad spectrum of global providers. Businesses around the world including Alipay, Microsoft, Stripe, and Airbnb leverage our product suite to increase approvals of more good transactions, reduce customer friction at account opening, and find fraud.

Contact us to learn more.https://ekata.com | 1.888.308.2549