THE VALUE OF

Pre-Authorization Screening

IN THE

Payments Ecosystem of Today

Pre-Authorization Screening
Solving Payment Challenges

EKATA

Table of Contents

Introduction

Timing is everything in comedy, life, and even online payments. Key stakeholders in the online payments ecosystem are rethinking the way payments are processed, with a renewed emphasis on linking digital identity back to the human behind the transaction during the pre-authorization stage. The powers that nudged the pendulum of focus toward the customer might not be as straightforward as you might think.

Technology continually evolves the way we do business, digitally transforming operations and processes, but they also present a double-edged sword for the payments industry. On the one hand, they open up opportunities to create new and exciting products and engage in better customer experiences. On the other hand, they are like a moth to a flame, enticing cybercriminals to take advantage of gaps in new platforms and processes.

Cybercriminals never sit on their laurels, and as digital payment systems have evolved, so have the fraud attacks. Scams and complaints to banks about fraud increased by 43% in 2017[1]. In the United States, 80% of organizations have seen online fraud losses increase from 2017 to 2018[2].

Never before in history have online payment processes had so many challenges to meet.

Recently, this landscape has been further impacted by the regulations that oversee the proper use of personal and financial data. Regulations such as the General Data Protection Regulation (GDPR) and Revised Payment Service Directive (PSD2) are re-shaping the online payments ecosystem. New innovations, around customer engagement in the form of open banking APIs and more robust security measures, can create a better payment environment that thwarts cybercrime. Never before in history have online payment processes had so many challenges to meet.

Innovation in the payment industry continues to delight consumers, offering a multitude of digital means to transact. But the need to authenticate these individuals, while complying with the newfound regulatory environment, is causing friction on the customer journey. This causes an imbalance as the race to payment authorization heats up, the tolerance for customer friction lowers, and the exposure to fraud increases.

To achieve the goals of new regulations, thwart cybercrime, and meet the needs of the customer, we need to innovate in how we authenticate payments too. Balance can be restored by leveraging Artificial Intelligence (AI) techniques such as Machine Learning (ML) and third-party data sources to verify good customers earlier in the transaction flow.

The phrase to sum up this new era of the smarter payments ecosystem is **be proactive rather than reactive**, starting with a layered approach to identity verification during pre-authorization screening.

[1] Which Magazine: https://www.which.co.uk/news/2019/05/fraud-complaints-hit-record-high-as-banks-new-anti-scam-measures-delayed/

[2] Experian, Global Identity and Fraud Report 2019: http://www.experian.com.hk/insights/2019-global-identity-and-fraud-report

SECTION 1

The Changing Landscape OF THE Payments Ecosystem

The Changing Landscape of the Payments Ecosystem

In the last 20 years, the internet has opened up global markets, robotic software is optimizing tedious repetitive tasks, and we have entered an era where digital transactions are an everyday norm. The World Payments Report 2018[3] has some eye-opening statistics that set the scene of this digitally transformed world of transactions. From this report:

Non-cash transaction volumes grew at 10.1% in 2016 to $482.6 billion (USD)

Non-cash transactions are expected to reach $726 billion (USD) by 2020

Debit cards transactions are growing by 14.7%; credit card transactions are growing by 10.9%

Non-cash transactions forecasted to have a CAGR (Compound Annual Growth Rate) of 12.7% globally; with emerging markets growing at 21.6% from 2016–21

The speed at which the payments world has changed has brought certain challenges. A number of global problems now plague the industry.

A comparison of Card Not Present (CNP) vs. Card Present authorization rates[4], sees the former at 82% with the latter, more established method, at 98%. The expected outcome is that CNP fraud is rising faster than Card Present fraud.

While CNP fraud is high and growing, customer confidence is being hit with false declines. In 2018, there were $331 billion (USD) of such declined transactions according to a Javelin study[5]. A declined payment results in an unhappy customer, with 32% of the falsely declined consumers having stopped shopping with that merchant.

A serious imbalance in the payments ecosystem has appeared: False positive decline rates are 3x the rate of existing card fraud. When customer experience is impacted, customers are lost.

How has the payments ecosystem become so complicated?

[3] World Payments Report 2018: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf

[4] Mastercard: OCTOBER 2017 THROUGH SEPTEMBER 2018 DATA, ACROSS ALL CARD TYPES, 2018

[5] Javelin: https://www.javelinstrategy.com/coverage-area/addressing-threat-false-positive-declines

A Brief History of the Payments Ecosystem

Many countries are experiencing the era of the 'cashless society,' but how did we get here? Let's look back to the start of the electronic payment era.

The beginning – the Internet

The development of today's internet is where the road to cashless began. Without this, the means to have a CNP transaction culture wouldn't exist. But the beginnings of the internet are not, per se, of interest here. Instead, it is the development of the first online transactions that are of interest.

The 90s saw the ubiquitous rise of consumer interest in Internet websites. In 1993, there were 130 websites, and by 1997 there were over 1 million. In 1994, online payments were shored up when the Stanford Federal Credit Union became the first financial institution to offer online banking. This created a playing field for others to enter, with PayPal appearing in 1999[6]. The world of eCommerce had truly begun, and with this, the need for protocols business models to manage it.

Turning to face the changes

As the internet grew in popularity and as new models of doing business moved online, new modes of transacting appeared. Debit and credit cards had been around since the 1960s, offering a natural conduit between the real and the digital world.

New companies, such as Authorize.net (a Visa owned company), emerged to better facilitate online transactions. Online retailers such as Amazon and eBay were born, then PayPal linked directly with eBay, demonstrating just how seamless transactions could be. The age of the online payment gateway/processor had been established. By the 2000s, there were billions of transactions being handled via direct integration with payment gateways that then passed them onto processors. The environment was shaping up into the one we know today.

Online payments in the 21st century

Mobile devices and voice-activated assistants like Amazon Echo, allow customers to directly place orders. Customers are savvier in regard to their data privacy and security rights too, and the customer experience is critical in the complex web of multi-channel online transactions.

In 2019, the WeChat app was used to send a record-breaking 823 million monetary gifts called 'digital red packets' during New Year[7].

And now, in a bid to regulate this changing technology landscape and embrace modern customer expectations, we see new legislation and regulations.

[6] Internet Live Stats: https://www.internetlivestats.com/total-number-of-websites/

[7] ZDNet: https://www.zdnet.com/article/over-800-million-wechat-users-sent-digital-monetary-gifts-during-lunar-new-year/

Regulations and the Payments Ecosystem

The regulatory landscape is being driven to evolve and reflect the new challenges of our cashless society through customer expectations for a seamless experience, increased individual control over privacy, increased cyber threats and increased identity fraud.

Two key regulations are working to solve these challenges: Revised Payment Services Directive (PSD2) and General Data Protection Regulation (GDPR). We will look at both here.

Revised Payment Services Directive (PSD2)[8]

The Payment Services Directive (PSD) is a legislative framework established in the European Union (EU), designed to add elements of security and customer control to financial transactions. PSD was established in 2007, and as online payments technology has evolved, so have the elements of PSD. To reflect this evolution, the Payment Services Directive Version 2 (PSD2) was implemented in the EU on January 13th, 2018. This directive continues to be reviewed and revised to ensure alignment with the changing needs of the industry, and to this end, new authentication rules will be implemented in September, 2019.

The Elements and Implications of PSD2

PSD2 affects any entity that handles payments within the European Union, including organizations associated with EU banks or financial service providers, fintech companies and online merchants. The main areas that the updated legislation focuses on are:

- Improving the security of online transactions (Strong Customer Authentication (SCA))
- Facilitating third party access to financial accounts (Open Banking)
- Improved customer rights and surcharge handling

The more stringent security provided by SCA comes with more friction. Merchants and acquirers have to innovate to improve this situation or risk losing customers.

PSD2 and Strong Customer Authentication (SCA)

Security is a serious issue in online transactions. Mobile payments are stalling in some countries because of customer concerns over security[9]. PSD2 proposes to improve this situation by legislating around improvements in the authentication measures used during “customer-initiated” online payments. Within the EU, this will affect all online transactions that are done with a credit/debit card or as a bank transfer. There are several exceptions to this rule, such as ‘merchant-initiated payments,’ e.g. recurring direct debits and not contactless payments, and Transaction Risk Analysis (TRA) (see section four for further details about the TRA.)

[8] Payment Services Directive Version 2: https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366/law-details_en

[9] Simon Kucher and Partners:: https://www.simon-kucher.com/sites/default/files/2019-01/SimonKucher_Report_Payment%20Adoption_Final.pdf

The SCA rule aims to help in preventing identity theft and fraud, which are at an all-time high. Analysts at Juniper Research[10] estimate online payment losses, due to fraud, to be around $43 billion globally, by 2023, with 'synthetic identity' being a main driver.

The more stringent security provided by SCA comes with more friction. Merchants and acquirers have to innovate to improve this situation or risk losing customers.

PSD2 and open banking

PSD2 constitutes a true innovation in online payments in the form of 'Open Banking'. This initiative is revolutionary in encouraging banks to open up their services via an API, aka a programmatic interface. While open banking is not mandatory in PSD2, it is strongly encouraged. Banks in the European Union are already building these APIs, which include functionality to allow a merchant to request payments directly from a customer's bank account; the customer sitting in the middle of the transaction and authenticating the process between the merchant-bank.

Online merchants can offer more direct payment relationships using a Payment Initiation Service Provider (PISP). This relationship, managed through the customer, offers cost reductions, faster payments, and better customer relationships.

Surcharge Handling

PSD2 brings into effect a ban on certain types of surcharge. The scope of the ban focuses on consumer (B2C) payments but can also affect business (B2B) payments. The surcharge ban within PSD2 prohibits merchants from charging any additional fees if a consumer makes a payment using certain payment methods.

General Data Protection Regulation (GDPR)

The next regulation that has focused on the world of online data (and therefore payment transactions) is the General Data Protection Regulation (GDPR), again from the EU. This is also an updated regulation from an earlier directive the Data Protection Directive (DPD) first enacted in 1995.

The GDPR came into force on May 25, 2018, and although EU-centric, it has a far-reaching impact across the world. The GDPR has a wide-jurisdiction, which means that any organization that does business with an EU citizen in an EU member state must meet the requirements. The fines that come with non-compliance are the largest of their kind in the world and can be up to 4% of global annual revenue or 20 million euros, whichever is higher.

The GDPR is, again, about improving the lives of consumers. At its core, is the privacy of the data that is shared with online companies. A number of consumer rights are covered by the legislation. The GDPR sets out eight data subject rights:

[10] Juniper Research: https://www.juniperresearch.com/press/press-releases/losses-from-online-payment-fraud

1. be informed about your data;
2. have access to data;
3. ask for data rectification;
4. ask for data erasure;
5. request restrict processing;
6. have data portability;
7. object; and,
8. not to be subject to automated decision-making including profiling.

All come under the lawful basis umbrella of 'consent'. That is, consent freely given and granular, to allow data to be collected and processed as part of doing business with that customer.

GDPR + PSD2: a match made in consumer heaven

The combination of these two regulations provides even stronger and more stringent online transaction control. GDPR, being used to directly protect consumer rights in how their data is used, has become the guardrails to PSD2's introduction of open banking. This adds in a layer of protection to ensure an open banking environment is not abused by players in the ecosystem. And, both GDPR and PSD2 place an emphasis on securing access to consumer data.

The global spread of regulations

The EU may have started the online transaction and privacy ball rolling, but it continues to roll in other countries. The GDPR has affected organizations across the world. This has created an enormous amount of media coverage. At the same time, cybersecurity incidents like the Equifax breach of 2017 and the Facebook/Cambridge Analytica privacy debacle, have created a customer mood. Consumers across the globe now expect both a seamless and privacy-enhanced online transaction experience.

Some locations that are about to enact, or already have enacted, similar regulations to GDPR/PSD2, include:

California:

The California Consumer Privacy Act (CCPA) is often likened to the GDPR. It differs somewhat in the size of an organization it is aimed at, bringing an emphasis to larger companies. The jurisdiction of CCPA is about protecting consumers who are residents of California, USA.

Australia:

Australia is enacting the Open Banking framework, which has similarities to the PSD2 open banking initiative. Like open banking, it is based on API functions and requires robust multi-factor authentication for security. The Open Banking framework is part of Australia's Consumer Data Right (CDR) legislation which, like GDPR, gives consumers greater power to control their data.

Japan:

Japan's Personal Information Protection Act (PIPA) is overseen by the Personal Information Protection Commission (PIPC) - a Japanese supervisory authority. PIPA was enacted on May 30th, 2017 and is similar in some ways to the GDPR. For example, it is designed to protect the processing of personal data and sets out specific data subject rights around erasure and correction.

Regulations like PSD2 and GDPR and their counterparts in other areas of the world are not created in isolation. They are a result of change. Change in how we do business, change in technology to perform that business, and perhaps of most note, change in how customers expect to be able to transact online.

Mexico:

The Open Bank Project in Mexico is similar to PSD2 opening banking. It is expected to come into force by 2020. Like its European counterpart, it will allow for a more customer-centric banking experience. However, it is expected that the Mexican Open Banking standards will be wider and extend to all financial services.

Canada:

The Personal Information Protection and Electronic Documents Act (PIPEDA) is aimed at the private sector, for-profit, companies who process personal data and are not federally regulated. PIPEDA came into force on April 13, 2000 and covers the privacy of personal data when it is processed. PIPEDA has similarities with GDPR such as the right to access data and the right to challenge the collection of data.

Customer data and regulations across the global payments ecosystem

Regulations like PSD2 and GDPR and their counterparts in other areas of the world are not created in isolation. They are a result of change. Change in how we do business, change in technology to perform that business, and perhaps of most note, change in how customers expect to be able to transact online.

However, getting the balance of usability, security, and performance right, under the weight of legislation is possible with the right tools.

Timeline

- **1994 -** Stanford Federal Credit Union first online bank
- **1995 -** Data Protection Directive from EU (precursor to GDPR)
- **1997 -** Internet begins ubiquitous use
- **1999 -** PayPal starts up
- **2000's -** Billions of online transactions being handled
- **2007 -** Major U.S. banks develop mobile banking
- **2011 -** ePayments launched
- **2018 -** GDPR enacted
- **2018/2019 -** PSD2 comes into force (open banking and SCA)
- **2018/2019 -** Amazon Alexa skills to do online banking
- **2019 -** WeChat used to send 823 million 'red package' New Year gifts
- **2019 onwards –** Regulations across the globe mimic GDPR and PSD2

Conclusion

The changing landscape of technology is reflected in the online payments ecosystem, which is reflected in various regulations. This tripartite relationship is a continuous feedback loop, each informing the other to push for improved security and better customer experiences.

Regulations ensure that innovations like open banking have support from governments and industry. They are also there to ensure that these innovations are done within an environment of trust, security, and privacy.

PSD2, with its leap in innovation from open banking, modulates this with stronger security in the form of the SCA rule on authentication. Similarly, GDPR works to create a better, more controlled, user experience, when an online data transaction happens.

Where once the business needs of financial institutions came first, now society and customer expectations are placed center stage. While technology makes things easy and improves customer experience, regulations often play catch-up. This is what is happening in the regulation landscape today. As the regulations tighten up to reflect social change, our models of processing online transactions need to reflect this.

SECTION 2

How the Evovled Payments Ecosystem Impacts Each Stakeholder

How the evolved payments ecosystem impacts each stakeholder

As the online payment arena has evolved over the years, and as the technology landscape has become ever-complex, the payments ecosystem has matured. Regulations, like PDS2 and GDPR, have created a layer that presides over the top of this ecosystem to modulate its behavior. In this section, we will look at each of the main ecosystem players, their part in the whole, and the impact on each by regulations such as PDS2.

Stakeholder impact: customers

When the payments ecosystem is broken down into its constituent parts, the most important of those parts, and the pivot upon which everything turns, is the consumer. Regulation updates have reflected this position clearly. PSD2 and GDPR have a distinct user-centric focus.

The mantra of "the customer is king" has come to fruition by the driving forces of data protection and privacy regulations. To create a modern online payments ecosystem, the regulations continuously evolve and improve. With this evolution in mind, certain key requisites were given a spotlight, these being:

- Improved security: Insecure practices in financial and personal data have created a landscape that is a cybercriminals playground. The data security ecosystem has reached a breaking point with 14.7 billion data records stolen since 2013[11]. Updates to regulations have placed more focus on security measures to protect this data. PSD2 has enacted the SCA rule to ensure robust access control and GDPR mandates encryption and other security measures to protect data transactions.

- Improved privacy: Five years ago, privacy was something only discussed in specialist conferences. Now, privacy is a major topic for any organization that processes personal data, including financial information. The drivers for this debate have been the multitude of data breaches and poor privacy practices by major consumer platforms such as Google and Facebook. Consumers now expect online transactions to be respectful of privacy, and regulations like GDPR,CCPA, and PIPEDA, have provisions to specifically address this.

- More seamless transactions: Security and privacy are one side of a complex equation. The other side is usability. Customers want easy, fast, click-reduced transactions when they go through an online purchase. PSD2 and open banking are bringing opportunities for online merchants to provide more seamless customer experiences when paying for goods online.

- More choice in how to transact: Open Banking offers more choice to the customer and to the merchant. Customers can pay directly for goods via their bank, cutting out the middle-man. The merchant effectively becoming a PISP.

[11] Gemalto, Breach Level Index: https://www.breachlevelindex.com

Stakeholder Impact: Merchants

A 2019 report from PYMNTS.com and Ekata[12], pointed out that "only 25% of European online merchants are aware of the requirements under PSD2 for more robust and strong customer authentication."

The payments ecosystem is intrinsically cooperative and inter-linked, and merchants have to reflect the needs and expectations of customers, while also working within the confines of regulations that mandate robust security and privacy. The merchant is the face of the ecosystem, and as such, regulation will impact them in several ways:

- Strong Customer Authentication (SCA): PSD2 mandates increased levels of secure authentication - aka, customer friction - when processing an online transaction. This can be met using 3-D Secure (3DS) 2.0, or surpassed if exemptions such as Transaction Risk Analysis (TRA) are met (more on this later.)

- More direct customer interactions: PSD2 has brought the revolution of open banking to merchants who can directly link to bank APIs. This, in turn, allows customers to have more direct interactions with the merchant.

- Cost-reduced transactions: Using the payment options that open banking offer, means that the cost of an online transaction can be reduced.

- Surcharge bans: PSD2 bans certain surcharges, and countries like the UK have banned any charges from being added to transactions. Thus, profit margins will be tighter than ever.

- Impacts in areas such as loyalty and reward schemes: Many schemes, especially larger ones, will be required to include country-specific registration.

- Faster complaint handling: PSD2 has cut the time to deal with a customer complaint from 8 weeks to 15 days.

Underpinning these changes is the continued need to have more customers. The changes afoot in the online payments ecosystem, due to global regulations, now place enhanced focus on the merchant to provide exceptional customer experiences.

Stakeholder Impact: Merchant Acquirers/ Payment Service Providers (PSPs)

PSD2 widens the scope to create new types of payment providers. One UK retail bank has sent a warning out, explaining that changes in the online payment regulations could mean £20m (GBP) per annum of lost revenue, if the 10 biggest retailers become authorized as a PSP[13]. The scope of the PSP is now wider under the remit of PSD2, increasing opportunities for innovation and transparency.

Under PSD2, 3rd party facilitators of the ecosystem become Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs).

[12] EKATA,, The PSD2 Tracker, April 2019: https://www.pymnts.com/tracker/psd2-april-2019-tracker

[13] PWC: https://www.pwc.co.uk/industries/banking-capital-markets/insights/psd2-a-game-changing-regulation.html

The PSP offers a new and crucial role in online payments as the security enforcer of the ecosystem:

- Security and risk: The new role of the PSP is to help merchants with fraud prevention, to provide a good customer experience and improve the overall security of the ecosystem:

- SCA exemptions: Under the Transaction Risk Analysis (TRA) exemption, PSPs may bypass SCA for remote transactions, provided that risk analysis is applied and the PSP's fraud rates and transaction amounts are under certain thresholds (Article 18 of the RTS). This offers a key opportunity for the PSP.

PSPs must embrace technology to keep up and retain market share. The PSP is no longer just a money mover. They must innovate around security and fraud to find their fit in this new, more flexible, ecosystem. The PSP must differentiate on value vs. just processing fees.

Stakeholder impact: issuers

A recent survey by Accenture[14], found that 85% of banks are developing open banking technology and 90% believe it will boost organic growth. However, modern banks operate within an increasingly sophisticated cybercrime environment, and this needs to be tackled. Issuers, such as banks, have taken on the challenges and the opportunities that PSD2 affords them to fix these problems. PSD2, using open banking and the SCA rule, opens opportunities to review how an issuer approaches fraud and risk management.

- Potential friction issues: The implementation of the robust authentication required by the SCA rule may mean increased customer friction. The new 3-D Secure (3DS) 2.0 system can help to reduce this friction by moderating a transaction using a version that has 'frictionless flow' for certain levels of payment. However, higher levels of payment will still be required to use a 'challenge' type system that requires user input.

- Open banking pros and cons: Open banking can create innovative products to build customer relationships. However, it can also offer fraudsters new opportunities. Social engineering needs to be a consideration when designing a system based on open banking APIs.

- Competition: Issuers need to innovate to keep up to date with the buoyant Fintech community and take on agile Fintech unicorns. A survey by Fujitsu Financial Services found that 37% of bank customers would switch to another if they were not offered the latest technology to engage[15].

There are many positives in keeping up to date with technology, and PSD2 offers a wake-up call to the issuer community to keep pace with change.

[14] Accenture: https://www.accenture.com/_acnmedia/PDF-77/Accenture-Brave-New-World-Open-Banking.pdf

[15] Fujitsu Financial Services: https://www.fujitsu.com/uk/Images/fujitsu-european-financial-services-survey-2016-infographic.pdf

How the Payments Ecosystem is Tied Together

	Consumers	Merchants	Acquirers & PSPS
What they Need	Frictionless Experience Trust & Security	More Consumers Consumer Trust	More Merchants Optimized Risk Portfolio
SCA Challenge	Higher friction during checkout expeirence	Decrease in conversion rates for online payments	Merchants shopping around for alternatives

SECTION 3

Challenges for the Online Payments Ecosystem

Challenges for the online payments ecosystem

Insights and Actions

Online commerce is moving at a rapid pace that is much faster than its historical retail counterpart. Major technological advancements have created a world of instant, frictionless payments on goods/services that are immediately delivered to the customer. The result is a maturing of customer expectations: our customers now demand an experience that is clean, swift, and without failure. The 'instant gratification' culture is being fed by services like Amazon Prime Now which offers authentication, authorization, and home delivery in as little as an hour after an order is placed.

Online payments have become the pivot in the payments ecosystem; fitting the payment model to the customer expectations within this climate of fraud, results in:

- An increasingly cross-border ecosystem
- Poor authorization rates and false declines
- Unknown territory and lack of technical readiness

Let's look at each of these in more detail.

Increasingly cross-border

The modern system of online payments is a result of the globalization of eCommerce afforded by the internet. Cross-border payments present new challenges for stakeholders in the ecosystem, and the projected growth of cross-border commerce is staggering. According to a recent study, cross-border commerce is growing 2X faster than domestic, with a 3X market growth rate expected (from $300 billion in 2015 to $900 billion in 2020.)[16]

Despite this, the regulations do not attend to the needs of border-less transactions. PSD2, for example, is specific to transactions that are Europe to Europe only. This lack of coverage for cross-border transactions on a global scale, will open up new opportunities for fraudsters and cybercriminals; one thing that is assured in the world of fraud is that cybercriminals will take advantage of any gaps.

It is clear that the emerging regulatory landscape is moving across the globe, and 'mimic regulations' that follow the lead of GDPR and PSD2 are appearing. Being a first-mover in the areas that these regulations cover, will give online payment stakeholders a competitive edge when new regulations enter their jurisdiction.

Poor authorization rates and false declines

The antiquated way of performing online payments involved using asynchronous fraud assessment of the transaction itself. This was slow and cumbersome, and therefore unable to meet the time compressions expected by stakeholders. A business could easily lose a customer because of a poor-quality experience caused by slow responses and false declines – that is a customer being falsely rejected.

[16] DHL: https://www.dhl.com/content/dam/downloads/g0/press/publication/g0_dhl_express_cross_border_ecommerce_21st_century_spice_

Globally, the problem caused by asynchronous fraud assessment has plagued the online payments industry. Below are some statistics that spell out the issues:

- Poor Authorization Rates: 82% authorization rate for Card Not Present (CNP) vs. 98% authorization rate for Card Present
- Increasing Fraud: CNP fraud is rising quickly, with Analyst Firm, Juniper Research, predicting CNP fraud costs to reach $130 billion by 2024[17]
- False Declines: result in lost and disgruntled customers
  - $331 billion lost due to false declines of good transactions in 2018
  - 32% of falsely declined consumers stop shopping with the merchant
  - False positive decline rate is 3x the rate of existing card fraud

This has created a clear disconnect. The authorization rails of the older payments system were simply not built to accommodate the online payments world that exists today.

There are a number of reasons why the authorization rate problem exists. One of the key reasons is the lack of fluid data sharing between entities in the payments value chain (merchants, acquirers, card schemes, and issuers). Data sharing in a risk-managed, privacy-enhanced and secure manner, is the fuel behind the modern online payments ecosystem. The result of this poor fluidity, is that risk decisions are made in a vacuum, where:

- Merchants are forced to make risk decisions on data from the shopping cart
- Issuers make risk decisions on data from cardholder account and spending patterns

Unknown territory and lack of technical readiness

The evolving ecosystem is moving into unknown territory. This is a cold start problem that requires the right solution for the ecosystem to sustain and innovate. Not only are new patterns of fraud emerging, but as regulations catch up, there is also a liability shift in terms of who owns 'fraud.'

This is compounded by a lack of technical readiness across multiple key ecosystem stakeholders, when it comes to complying with emerging regulations. Issuers, in particular, are struggling to meet the evolving needs of the modern online payments ecosystem.

As the regulatory landscape has shifted, so too, has the liability. Online payment stakeholders who previously had no fraud responsibility footprint, now have to comply with the stringent requirements of PDS2 elements and Strong Customer Authentication (SCA).

[17] Juniper Research: https://www.juniperresearch.com/press/press-releases/retailers-to-lose-130-billion-globally

SECTION 4

NAVIGATING THE LANDSCAPE TO CREATE A BETTER ONLINE PAYMENTS ECOSYSTEM FOR TODAY AND TOMORROW

Navigating the landscape to create a better online payments ecosystem for today and tomorrow

Balancing fraud prevention with customer experience to improve overall portfolio performance

The evolution of commerce and the online payments ecosystem have opened up more opportunity than ever for fraudsters. The business of fraud is enormous and ever-increasing; in the UK alone, financial fraud increased by 78% in 2018 and these types of figures are not unique to the UK. Drivers for increasing fraud include social engineering and account takeovers.

As fraudsters evolve to jump technological barriers, we need to up our game. This translates to being flexible and dynamic in our technology choices to win this war of attrition.

The flipside of the coin is providing excellent customer experiences, which is arguably even more important in today's landscape. Customers are being lost because of the fear of fraud. Only by understanding how to balance security with usability can we, as an industry, solve the expectations of the new paradigm in online payments with the requirements of the new regulations.

Reducing customer friction through exemptions like Transaction Risk Analysis (TRA)

Help in compliance with certain regulations, like PSD2, does exist in the form of exemptions such as Transaction Risk Analysis (TRA). However, expectations can also come with such exemptions. In meeting the TRA exemption, for example, stakeholders must comply with low fraud rates as shown in the table below:

Exemption Threshold Value	Remote card-based payments
€500	<0.01
€250	0.01 - 0.06
€100	0.06 - 0.13
0-€30	Exempt

The point of the TRA exemption being that in order to provide low-friction customer experiences, fraud rates must be kept low.

Another consideration is that chargebacks are no longer a free-pass; **fraud rates must be kept low for the entire network/portfolio.**

[3] World Payments Report 2018: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf

[4] Mastercard: OCTOBER 2017 THROUGH SEPTEMBER 2018 DATA, ACROSS ALL CARD TYPES, 2018

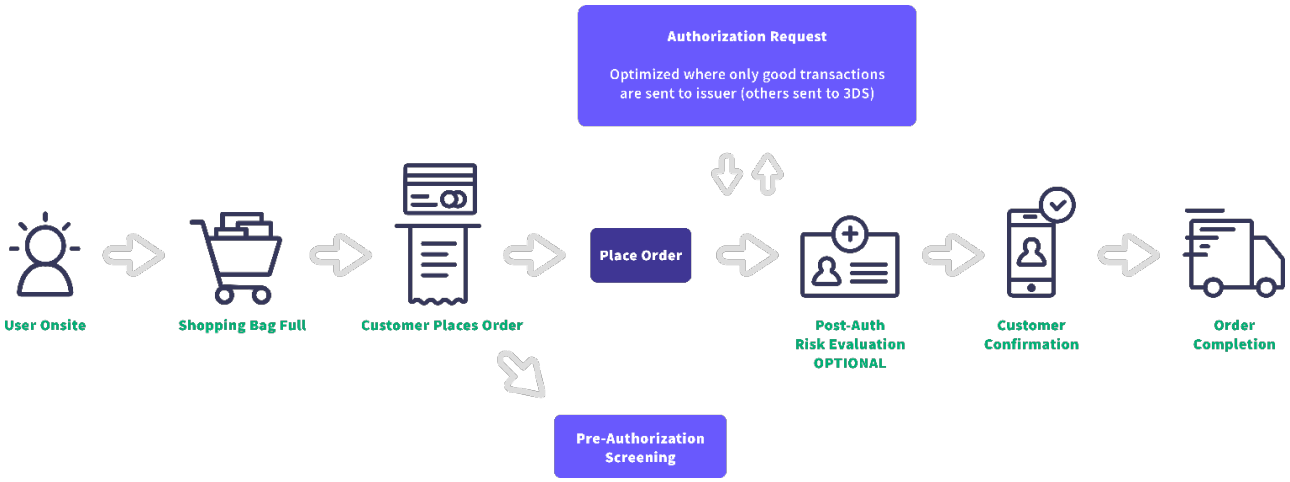
[5] Javelin: https://www.javelinstrategy.com/coverage-area/addressing-threat-false-positive-declines

With the right technology measures in place, especially around authentication, the ecosystem will become a place of innovation, competitive edge, and great customer experiences.

Defining "pre-authorization"

Before continuing, what exactly do we mean when we say "pre-authorization?"

Definition of pre-authorization (according to Ekata): time period after payment details have been submitted, and before sending to issuer for authorization request.



A layered approach to pre-authorization screening

The online payments ecosystem is in constant upheaval from changing technology and societal expectations. The challenges this brings require a modern response that balances fraud prevention with excellent customer experiences. The key to making the ecosystem work for all stakeholders is to turn inaction into action; using technology to enable your organization to be proactive rather than reactive. Part of this shift includes a fresh focus on the pre-authorization portion of the transaction flow.

Taking a layered approach to pre-authorization adds a dynamic layer to help prevent fraud and improve customer experience. Adding intelligent identity verification earlier in the transaction flow of an online payments ecosystem moves the pendulum towards more secure, balanced processes.

The key to successful pre-authorization screening is in the timing and the intelligent use of data. Furthermore, combining these dual forces balances risk with smooth customer transactions. Applying pre-authorization screening helps to counterbalance the challenges that the evolved ecosystem and regulatory environment have created. Using pre-authorization allows us to build bridges across security, privacy, and customer experience.

[3] World Payments Report 2018: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf
[4] Mastercard: OCTOBER 2017 THROUGH SEPTEMBER 2018 DATA, ACROSS ALL CARD TYPES, 2018
[5] Javelin: https://www.javelinstrategy.com/coverage-area/addressing-threat-false-positive-declines

Benefits of pre-authorization screening

Aside from general improvement in the overall downstream workflow of a transaction, pre-authorization screening offers a number of benefits in use. The key overall benefit is improved consumer experience, and includes:

- A reduction in false declines
- Better checkout experiences
- Improved conversion rates
- Decreased abandonments
- Fewer orders sent to manual review

In the context of the emerging regulatory environment, pre-authorization screening has become a requirement for any sophisticated player in the space, offering help by:

- Keeping overall fraud rates low, which in turn offers exemptions such as Transaction Risk Analysis (TRA)
- Removing the need to send good customers through 3DS (which could lead to a "step-up" challenge and increased friction)
- Increasing authorization rates using "Trusted MID" (if a merchant/acquirer sends fewer suspected fraudulent transactions through authorization rails to the issuer, the issuer will naturally approve more transactions from that merchant/acquirer)

What is required to build a layered approach to pre-authorization screening?

Historically, businesses relied solely on internal data and signals such as blacklists, shopping cart data, customer history, etc. during the pre-authorization portion of the workflow. This was largely due to the lack of availability of third-party data sources. In addition, third-party sources were not involved in the pre-authorization screening flows, as most were not API-based, and were thus too latent to meet the need for a fast and economical model. The result was an inability to meet the volume and latency demands within an environment of increasing transactions and compressed time window expectations.

However, Artificial Intelligence (AI) techniques like Machine Learning (ML) have facilitated innovation to provide the accuracy, speed, and scalability needed to achieve this balance.

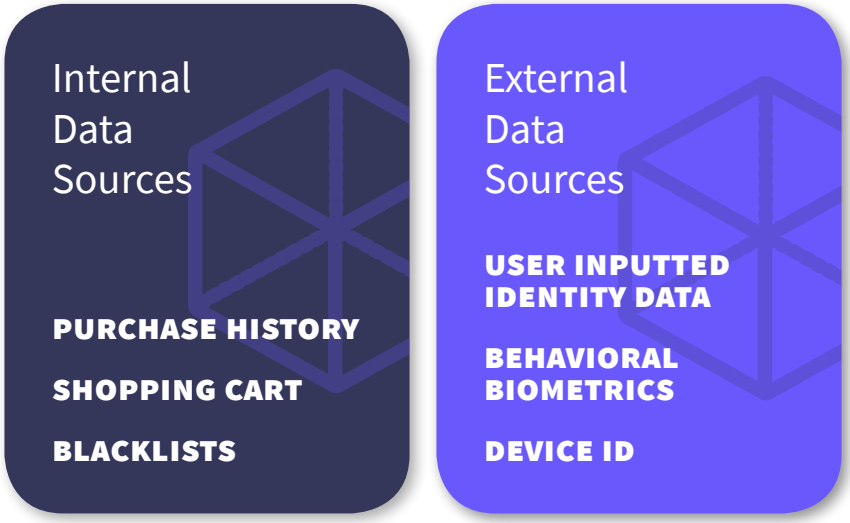
That being said, any successful ML model requires clean, accurate data to power it, and the more data a model can ingest, the better the performance. Third-party data sources are now an integral part of the pre-authorization workflow.

However, pre-authorization cannot rely on a single external data source. Instead, a layered approach is needed for detection and authentication early in the transaction flow. The types of third-party data used in a sophisticated pre-authorization approach can include:

- Device ID: this can work to identify both good and bad actors

[3] World Payments Report 2018: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf
[4] Mastercard: OCTOBER 2017 THROUGH SEPTEMBER 2018 DATA, ACROSS ALL CARD TYPES, 2018
[5] Javelin: https://www.javelinstrategy.com/coverage-area/addressing-threat-false-positive-declines

- Biometric data: this reveals the user behind the device
  - The real power of biometric data is understanding the profile of a user. Behavioral biometrics can, for example, identify account takeover.
  - User data verification - identity verification data, such as email address, IP address, phone number, home address, name



Transaction Risk API - the speed, accuracy, and availability needed

Third-party identity data analysis of name, phone, address, email, and IP play a vital role in today's pre-authorization screening. Ekata's Transaction Risk API was built specifically for low-latency pre-authorization models, and is designed to link digital identity back to the human operator in under 80ms.

The intelligent use of this data is also of key importance. Feature development for machine learning models provides payment fraud detection that is predictive and proactive. This is not possible using older, static, rules-based systems.

Additionally, access to data on a global scale is important in an environment that is cross-border for ecosystem stakeholders.

Speed is also of the essence in allowing for timely risk decisions keeping the customer experience smooth. Fast delivery of data (in less than 100 milliseconds) is fundamental, as pre-authorization checks are real-time and synchronous to the payments experience.

And last, but not least, these tools must be priced economically, as they will be used across all transactions – Ekata makes it fiscally possible to call third-party data and use it smartly on a massive scale.

[3] World Payments Report 2018: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf
[4] Mastercard: OCTOBER 2017 THROUGH SEPTEMBER 2018 DATA, ACROSS ALL CARD TYPES, 2018
[5] Javelin: https://www.javelinstrategy.com/coverage-area/addressing-threat-false-positive-declines

Conclusion

In past models of online payments, the validity of the identity behind a transaction was done later on in the payment flow of a transaction; most identity checks being performed post-authorization. This model needs to change to take on the challenges of fraud whilst improving customer experience. The key is to change the timing of those authorization checks to make them proactive rather than reactive. This will open up a more dynamic and flexible model of interaction between the ecosystem players.

As social and regulatory changes push for more thorough checks to be done upfront, the evolution of technology is facilitating this change. Customer data, the fuel in the payments ecosystem, is incredibly useful when companies take a layered approach to identity verification – drawing in from different places and applying intelligent methods of analysis. Internal data, biometrics, device ID, etc. are lightweight enough to be used in pre-authorization checks, especially when latency requirements are tight. Timing identity verification to occur 'pre' rather than 'post' authorization opens up new pathways. These new journeys can provide the balancing act needed to keep in compliance with regulations like PSD2 whilst ensuring that customer experience is seamless.

The ecosystem players, aka, the PSPs, online merchants, acquirers, and customers have sophisticated needs with the ultimate problem in the industry being acceptance. Merchants, PSPs, Card Schemes, and Issuers all benefit from accepting more transactions.

Smart identity data analysis is part of a wider puzzle to keep up with the evolving online payments landscape. Bringing the pieces of the payments jigsaw puzzle together, starting with a change from post to pre-authorization checks of a customer, will allow the payments ecosystem to blossom – balancing the needs of the customer against the threat of cybercrime. Layering the requirements of regulations like PSD2 onto the system helps to design payment processes that work for all.

The tools to solving this are at hand. Ekata has recognized this evolution, and turned lightweight data into smart data using AI and pre-authorization checks. Ekata is seeing a major shift in the industry - it is no longer just about reducing risk, but instead about helping merchants reach maximum performance.

About EKATA

Ekata (formerly Whitepages Pro) 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-time transactions 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.