



# Payment Fraud Risk Assessment

Review your exposure to payment fraud and develop strategies to keep your business safe.



# Contents

Why analyse your risk of payment fraud? .....	3
The payment fraud risk assessment framework. ....	4
Step 1: Identify the risks .....	5
Step 2: Quantify the risks .....	7
Step 3: Respond to the risks .....	25
Step 4: Monitor, Review and Report .....	29
PayPal's approach to risk and fraud management .....	31

# Why analyse your risk of payment fraud?

Payment fraud and cybercrime is a well-organised and global concern where fraudsters use dark web, crime-as-a-service functions to target businesses of all scales, all around the world.

As criminals get more sophisticated, businesses need to stay ahead or risk being steadily more exposed and suffering greater losses.

It's not just the lost revenue that costs businesses. There's the time and cost of dealing with incidents. Then there's the intangible cost of lost consumer confidence and possible damage to your business reputation.

Unfortunately, online fraud is unavoidable, but you can minimise its impact by taking a structured approach to identifying each area of risk, assessing its likelihood and potential impact, and defining an acceptable response. Those are the main elements of a payment fraud risk assessment, and this guide will help you get started.

**US\$1 trillion**

is the annual cost of global cybercrime.<sup>1</sup>

**4 in 10**

businesses lost at least 6% of revenue to payment fraud in 2020.<sup>2</sup>

**3.3x**

Every dollar lost to fraud costs around 3.3 times as much in time and other expenses.<sup>3</sup>

1. Center for Strategic & International Studies (2020), [The Hidden Costs of Cybercrime](#).

2. FIS Worldpay (2021), [Global Payment Risk Mitigation](#).

3. LexisNexis (2020), [2020 True Cost of Fraud Study – E-Commerce/Retail Report](#).

# The payment fraud risk assessment framework

Payment fraud comes in many forms. Some types of fraud are more common in different industries or in different countries. Following this framework will help you robustly analyse the risks faced by your business.

In Step 1, you'll start by identifying all the different areas of payment fraud risk faced by your business. Step 2 is where you analyse each risk to assess its potential impact on your business. In Step 3, we'll look at developing strategies to mitigate those risks and, finally, in Step 4 we'll create a structure to continually monitor and report on each area.



**01 Identify the risks**



**02 Quantify the risks**



**03 Respond to the risks**



**04 Monitor, review and report**



Step 01

# Identify The Risks



## Step 01

# Identify the Risks

Start by thinking about the following common types of fraud risk. Consider whether your business has any potential exposure to each of these.

Fraud	Level of business exposure		
	No exposure	Moderate exposure	High exposure
Credit card fraud			
Chargeback fraud			
Phishing / account takeover			
Friendly fraud			
Card testing			
Affiliate fraud			
Risks arising from data breaches			
Revenue loss through poor customer experience			
Revenue loss because of false declines			
Other payment fraud risks			
Other risks identified			
1.			
2.			
3.			
4.			

Step 02

# Quantify The Risks



**Step 02**

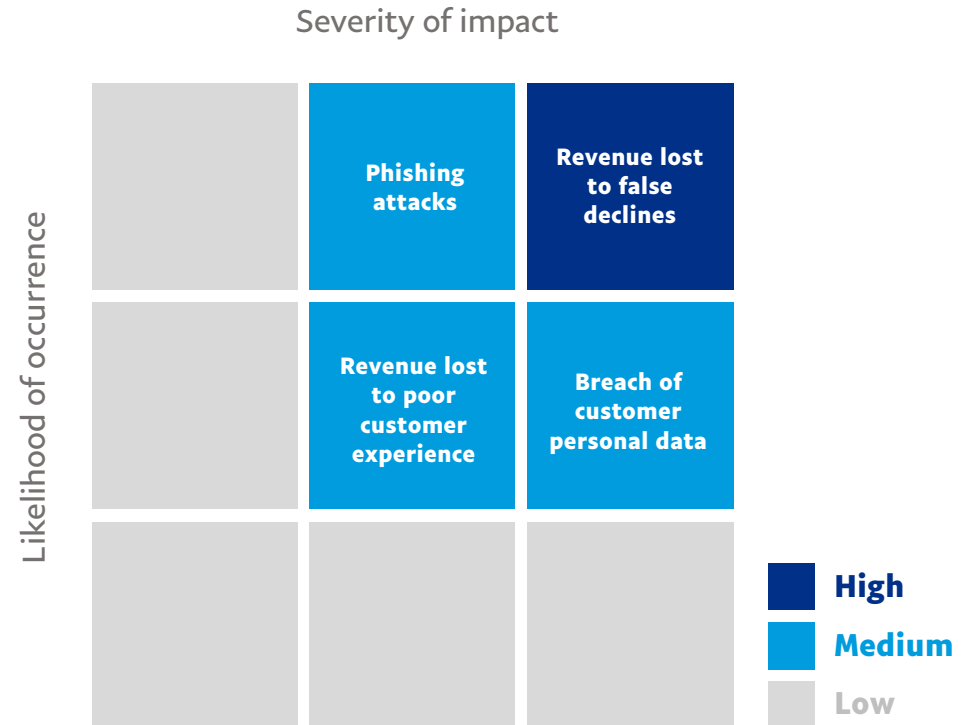
# Quantify the Risks

Now that you've identified the potential risks that your business faces, let's estimate how much they could affect your business.

**We need to look at two dimensions:**

- How likely it is that the event will occur, and
- How severely the business would be impacted if the event did occur.

We'll look at each risk in turn before bringing them all together in a risk assessment matrix, like this example.



(Note that risks listed here are only illustrative and may be different, or in different positions, for your own business.)

**The following sets of questions are intended to help you consider each risk in turn to decide where it sits within the risk assessment matrix.**

**You may find the following sources of information useful as you review and assess each risk.**

### Industry data

What is the prevalence of each type of risk within your business sector?

### Characteristics of your business

Consider how the way your business operates makes it more or less susceptible to fraud:

- Do you have high volumes of low-value transactions or fewer high-value ones? Higher value goods may be more attractive to fraudsters.
- Is your customer base domestic or international? It can sometimes be more challenging to detect fraud from overseas customers.
- What are the demographics and behaviours of your customer base? It's important to balance risk with customer experience. For example, younger, fast fashion customers will have less patience with a checkout process that is safe but slow and cumbersome.

### Transaction history

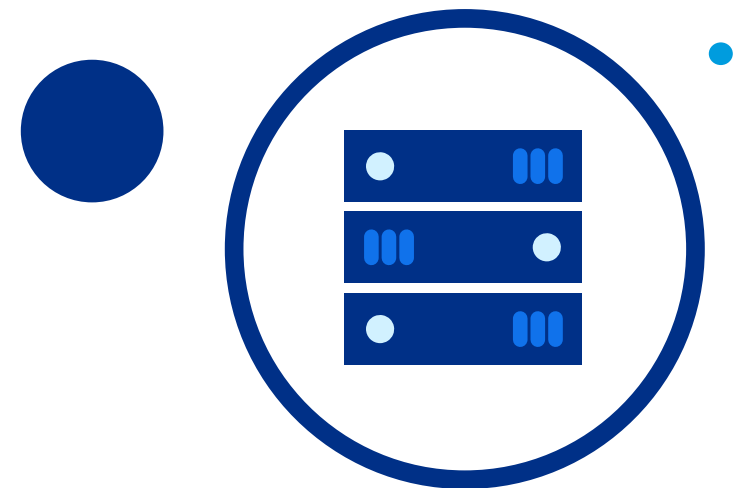
Past history may be a good indicator of your risk exposure. For example, has your business had a high proportion of chargebacks in the past? Is the trend increasing or decreasing?

### Insights from your payment processor

Your payment processor may be able to help you with performance insights for your own business and its sector.

### Payment industry insights

Reports and analysis from payment specialists like [PayPal](#) can also provide useful insight. As you assess the impact of risk, be sure to include any criminal or regulatory liabilities and background issues such as the financial condition of your business. For different risks, you may find it useful to consult with your finance and IT teams.



# Credit card fraud

01

What percentage of your online transactions turn out to be fraudulent? (Note, the global average for card-not-present fraud is 10–13%.<sup>4</sup>)

- < 10%     10 – 15%     > 15%

02

What is the historic cost of managing credit card fraud within your business? (Note that, on average, enterprises spend 10% of their ecommerce revenue managing payment fraud.<sup>5</sup>)

- Low     Medium     High

03

What is the historic trend of credit card fraud in your business?

- Decreasing     Stable     Rising

04

What is the trend for credit card fraud in your industry?

- Decreasing     Stable     Rising

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low     Medium     High

**How would you rank the Severity of this risk for your business?**

- Low     Medium     High

<sup>4</sup>. Vesta (2021).

<sup>5</sup>. Cybersource (2021), [2021 Global Fraud Report](#).



# Chargeback fraud

## 01

What percentage of your online transactions lead to a chargeback? (Note, the regional averages for chargebacks are: 3.8% in LATAM, 3.6% in APAC, 2.6% in Europe and 2.2% in North America.<sup>6</sup>)

- Less than 3.5%
- 3.5 – 4.0%
- More than 4.0%

## 02

Level of chargebacks is one of the measures used by payment processing companies to assess business risk. Has your payment provider expressed any concern about chargeback levels within your enterprise?

- No
- Yes

## 03

What is the historic cost of chargebacks to your business?

- Low
- Medium
- High

## 04

What is the historic trend of chargebacks within your business?

- Decreasing
- Stable
- Rising

## 05

How does this compare with the trend for your industry?

- Better
- About the same
- Poorer

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low
- Medium
- High

**How would you rank the Severity of this risk for your business?**

- Low
- Medium
- High

<sup>6</sup> Cybersource (2021), [2021 Global Fraud Report](#).

# Phishing/Account takeover fraud

01

How would you rank the occurrence of phishing fraud within your business?

- It is not one of our top five most frequent fraud attacks.
- It is one of our top five most frequent fraud attacks.
- This is our most common type of fraud attack.

02

What is the historic cost of this risk within your business?

- Low
- Medium
- High

03

What is the historic trend of phishing attacks in your business?

- Decreasing
- Stable
- Rising

04

What is the historic trend of phishing attacks in your industry?

- Decreasing
- Stable
- Rising

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low
- Medium
- High

**How would you rank the Severity of this risk for your business?**

- Low
- Medium
- High



# Friendly fraud

01

What percentage of orders turn out to be friendly fraud within your business? (Note, the regional averages for friendly fraud are: 1.6% in LATAM, 1.5% in APAC, 1.3% in Europe and 1.0% in North America.<sup>7</sup>)

- < 1.3%    1.3% - 1.8%    > 1.8%

02

What is the historic cost of friendly fraud to your business?

- Low    Medium    High

03

What is the historic trend of friendly fraud in your business?

- Decreasing    Stable    Rising

04

How does this compare with the trend for your industry?

- Better    About the same    Poorer

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low    Medium    High

**How would you rank the Severity of this risk for your business?**

- Low    Medium    High

<sup>7</sup> Cybersource (2021), [2021 Global Fraud Report](#).



# Card testing fraud

01

How would you rank the occurrence of card testing fraud within your business?

- It is not one of our top five most frequent fraud attacks.
- It is one of our top five most frequent fraud attacks.
- This is our most common type of fraud attack.

02

What is the historic cost of card testing fraud within your business?

- Low
- Medium
- High

03

What is the historic trend of card testing fraud in your business?

- Decreasing
- Stable
- Rising

04

What is the historic trend of card testing within your industry?

- Decreasing
- Stable
- Rising

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low
- Medium
- High

**How would you rank the Severity of this risk for your business?**

- Low
- Medium
- High



# Affiliate fraud

01

What percentage of your advertising budget is lost to affiliate fraud? (Note, according to Forrester, 69% of brands spending \$1 million per month reported that at least 20% of their budgets were being lost to digital ad fraud.<sup>8</sup>)

- < 15%     15 – 25%     > 25%

02

What is the historic cost of affiliate fraud within your business?

- Lower than current
- About the same as now
- Higher than current

03

What is the industry trend for affiliate fraud?

- Decreasing     Stable     Rising



Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low     Medium     High

**How would you rank the Severity of this risk for your business?**

- Low     Medium     High

<sup>8</sup>. Business of Apps (2021), [Ad Fraud Statistics \(2021\)](#).

# Risks arising from data breaches

For this question, you may wish to consult with your company's CIO and/or Data Controller.

01

Is your business compliant with data protection and privacy legislation in your target markets (such as the European Union's GDPR, Singapore's PDPA and Brazil's LGPD)?

- Yes, we are confident we comply with relevant legislation in our target markets.
- We are compliant with local legislation and that of our main markets, but not sure about other markets.
- We need to do further work to be confident of our compliance.

02

How often has your business suffered from data or legislative breaches in the past?

- Never
- Rarely
- Too often

03

What is the potential reputational damage your business could suffer from a data or legislative breach?

- Low
- Medium
- High

04

What are the potential fines and/or regulatory action faced by your business in the event of a data or privacy legislation breach?

- Minimal
- Moderate
- Severe

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low
- Medium
- High

**How would you rank the Severity of this risk for your business?**

- Low
- Medium
- High



# Revenue lost through poor customer experience

01

Has your business measured the revenue lost through poor customer experience (CX) because of fraud prevention measures?

- Yes  No

02

To what extent can you attribute cart abandonment at the checkout stage to friction and poor CX?

- We do not see any correlation between checkout stage abandonment and customer experience.
- There is a moderate effect of friction and poor CX causing checkout-stage abandonment.
- Poor CX at the checkout stage is a serious cause of revenue loss for the business.

03

To what extent does checkout-stage friction result in customers not returning, thus reducing customer lifetime value (CLV)?

- We do not see any effect on customer retention or CLV arising from checkout-stage friction.
- There is a moderate reduction in CLV arising from checkout-stage friction.
- Checkout-stage friction is a serious cause of customer loss and lower CLV.

# Revenue lost through poor customer experience

04

Does your business's current fraud management solution give you the insight and control to balance risk against customer experience?

- Yes       No

05

Across your market, do you see customer experience becoming more or less important?

- Less important. Customers are more concerned with other factors such as price.
- About the same as before.
- More important. With greater choice, customers are demanding a better, more friction-free experience.

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low       Medium       High

**How would you rank the Severity of this risk for your business?**

- Low       Medium       High

# Revenue lost through false declines

01

What is your business's overall payment or order rejection rate? (Note, the global average rejection rate is 3.0% for domestic orders and 5.6% for international orders.<sup>9</sup>)

- < 3.0% of orders are rejected
- 3.0% – 7.0% of orders are rejected
- > 7.0% of orders are rejected

02

If you measure your rate of false declines / false-positives (i.e. automatically declining payments that are actually valid), what is your average rate? (Note that 60% of businesses estimate their false-decline rate to be between 1.1% and 5%.<sup>10</sup>)

- Our business does not measure false decline rate
- < 2% of our declined transactions are false declines
- 2% – 5% of our declined transactions are false declines
- < 5% of our declined transactions are false declines

03

Based on your order/payment rejection rate and the percentage of those rejections that were actually valid, what is the value of improving payment approval rates by just 1%?

<sup>9</sup>. Cybersource (2021), [2021 Global Fraud Report](#).

<sup>10</sup>. Aite Group, cited by Kount (2021), [What you need to know about false positives...](#)

# Revenue lost through false declines

04

Does your business's current fraud management solution enable you to adjust risk sensitivity to balance against business risk appetite and customer experience needs?

- Yes  No

05

Does your current fraud-prevention solution actively adapt and adjust based on trends within the data (i.e. does it use artificial intelligence and machine learning)?

- Yes  No

06

Does your current fraud-prevention solution actively learn and adapt to fraud trends based on an industry-wide data set (rather than being limited to internal data)?

- Yes  No

07

What is the historic trend of your payment/order rejection rates?

- Decreasing  Stable  Rising

08

What is the historic trend of your false decline rates?

- Decreasing  Stable  Rising

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

- Low  Medium  High

**How would you rank the Severity of this risk for your business?**

- Low  Medium  High





# Other payment fraud risks to consider

The payments landscape is changing quickly but criminals are always looking for new opportunities to steal money. As you consider the ways your business is exposed to payment risk, make sure you think about new payment options your customers may be adopting, such as Buy Now Pay Later (BNPL) and cryptocurrencies.

It's also useful to think more broadly about how fraud attacks might affect other business relationships such as the one with your payment provider.

The following questions will help you consider these emerging risks.



01

List the new or additional payment options your business has started to offer in the last 12 months (such as BNPL, cryptocurrency, etc).

- 1 .....
- 2 .....
- 3 .....

02

For each of these, what additional liabilities does your business bear (for example, default on credit, exposure to anti-money laundering regulations, changes in exchange rates and so on)?

- 1 .....
- 2 .....
- 3 .....

03

What is the industry trend for fraud related to each of these payment options?

- 1  Decreasing       Stable       Rising
- 2  Decreasing       Stable       Rising
- 3  Decreasing       Stable       Rising

# Other payment fraud risks to consider

**04**

List other business relationships that may be affected by your exposure to payment fraud (such as your payment provider, banks, suppliers, etc).

1 .....

2 .....

3 .....

**05**

For each of these, consider how your business relationship might be affected by your enterprise's experience of payment fraud (such as higher prices, more onerous terms and conditions, etc).

1 .....

2 .....

3 .....

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

**Low**       **Medium**       **High**

**How would you rank the Severity of this risk for your business?**

**Low**       **Medium**       **High**



# Other risks

Copy this general sheet and use it for other risks you have identified.

01

What is the historic occurrence of this risk within your business?

Low     Medium     High

02

What is the historic cost of this risk within your business?

Low     Medium     High

03

What is the historic trend within your business?

Decreasing     Stable     Rising

04

What is the industry trend?

Decreasing     Stable     Rising

Having considered your answers to the above questions, estimate how much this risk could affect your business in the following risk assessment questions.

**How would you rank the Likelihood of this risk affecting your business?**

**Low**     **Medium**     **High**

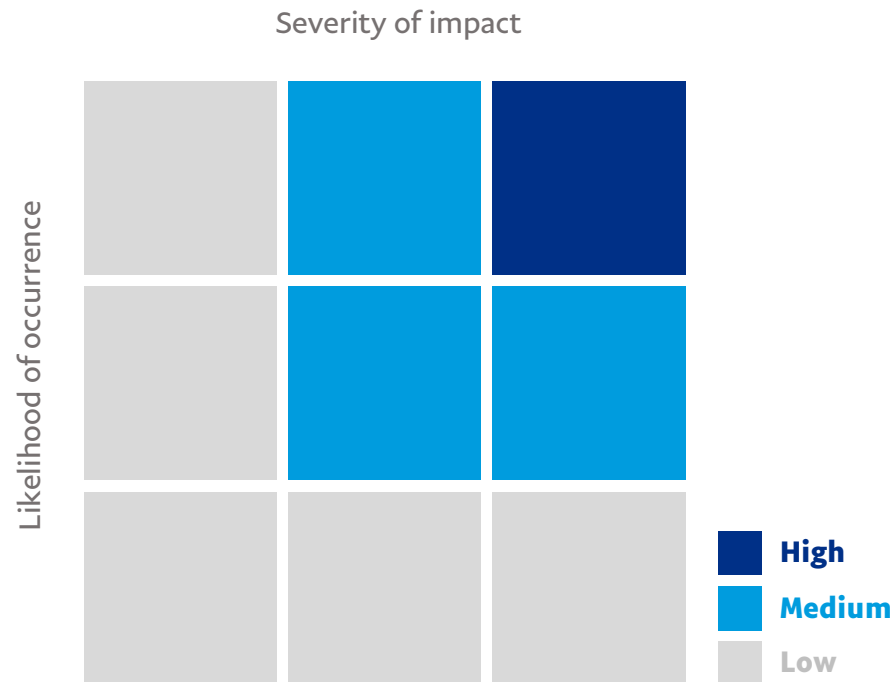
**How would you rank the Severity of this risk for your business?**

**Low**     **Medium**     **High**



# Bringing it all together

From the previous worksheets, bring together your rankings for Likelihood and Severity in this table.



Risk	Likelihood of occurrence	Severity of impact
Credit card fraud		
Chargeback fraud		
Phishing / Account takeover fraud		
Friendly fraud		
Card testing fraud		
Affiliate fraud		
Risk arising from data breaches		
Revenue lost through poor CX		
Revenue lost through false declines		
Other payment fraud risks		
Other risks...		

Now, plot the risks on this blank risk assessment matrix.

Step 03

# Respond to The Risks



## Step 03

# Respond to the Risks

Before developing strategies to respond to the risks identified in the previous section, it may be useful to consider the following questions.

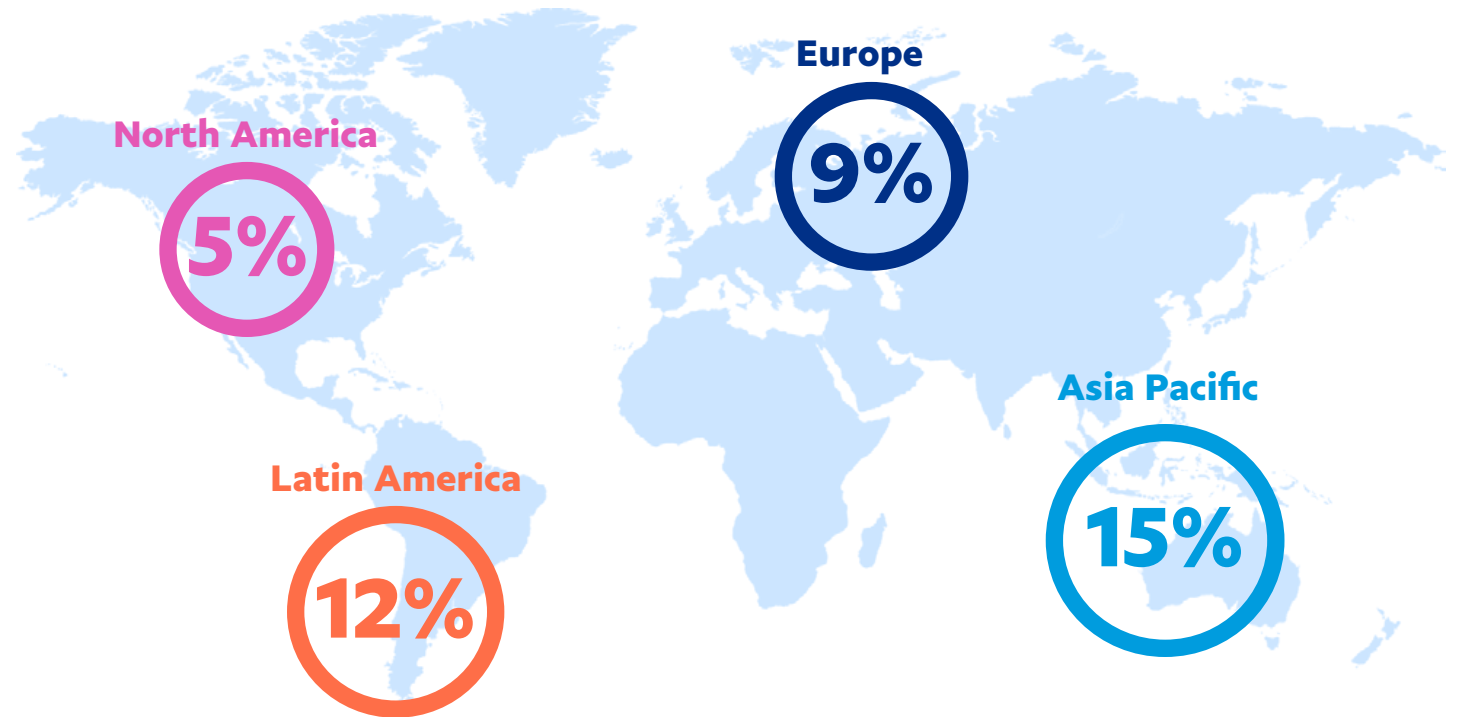
How important is fraud management to your overall business strategy?

- Extremely important
- Somewhat important

What percentage of your annual eCommerce revenue is currently spent managing payment fraud? (Note, the global average is around 10%.<sup>11</sup>)

- < 7%
- 7 - 13%
- > 13%

According to the Cybersource Global Fraud report<sup>12</sup>, enterprise-sized businesses spend an average of 10%. For all businesses, the regional averages are:



11, 12. Cybersource (2021), [2021 Global Fraud Report](#).

## Developing risk mitigation strategies

Based on your analysis, there may be some activities that you decide to terminate because the risk is too great. In other cases, the risk may be so small that you decide to do nothing and simply bear the small loss if it arises.

List those in the tables, here.

Activities to cease because the risk is too great

--

Low risk activities that do not require a mitigation strategy

--

For the remaining activities and potential risks, develop appropriate risk mitigation strategies. You may find that a single strategy addresses several risk areas together while others need a dedicated strategy.

The strategies you design will depend on the nature of your business, but you may find the following ideas useful.

## Review and revise customer data entry requirements

It is good practise to minimise the information you require a customer to enter when they set up a customer account. You should also enforce a strong password policy and use multi-factor authentication like 3D Secure.

For customer payments, consider offering a wide range of payment methods, including those (like [PayPal](#)) that do not require customers to enter their card and personal details onto your site.

## Review your payment technology

Many large enterprises manage payment technology in-house, often from several payment providers and built up over time. This can build risk and delay into payment processes resulting in poor customer experience, higher fraud rates and lost revenue.

It may be time to consider the advantages of switching to a single payment provider, like [PayPal](#), that can provide a wide range of payment options from a modular, easy-to-integrate, solution.

Updating your payment and fraud prevention technology may become a compelling strategy once you have quantified the risk inherent in older systems.

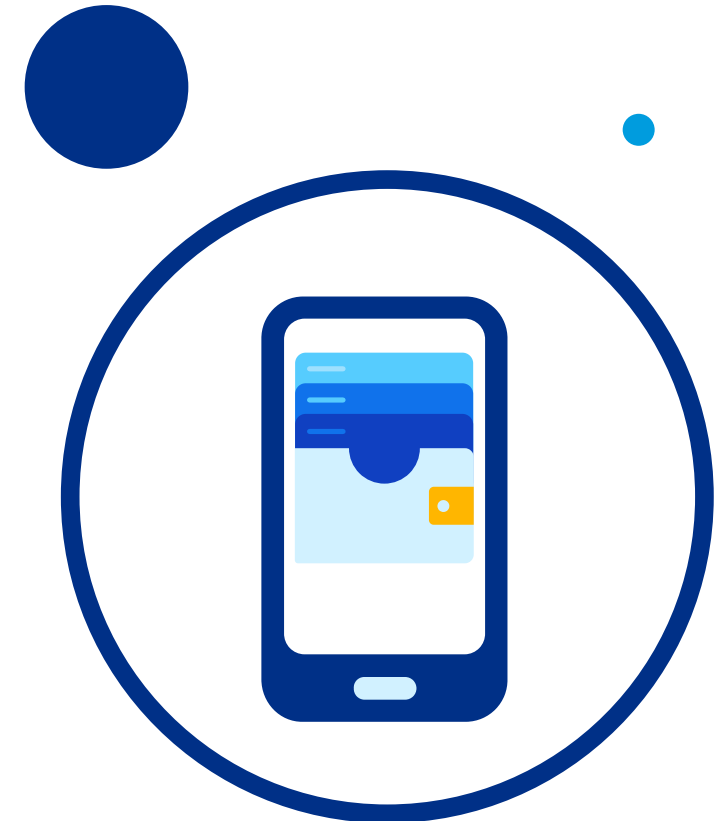
## Review your fraud prevention technology

Often, legacy fraud prevention tools have struggled to keep pace with the sophistication of today's international fraud industry and many businesses are moving to adaptive risk management solutions.

Powered by machine learning and, in PayPal's case, trained on huge volumes of real-time data, these solutions can be fast, agile and effective ways of managing fraud risk.

In the past three years, using its advanced fraud prevention technology, PayPal has been able to improve its global authorisation rate by more than 300 basis points (bps) for its branded processing. For new users signing up for PayPal, authorisation rates have been improved by an average of 600 (bps).<sup>13</sup>

Higher payment approval rates mean more revenue and happier customers for your business.



<sup>13</sup>. PayPal (2020), [How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates](#).



Step 04

# Monitor, Review and Report



**Step 04**

# Monitor, Review and Report

Once you have deployed your risk mitigation strategies and improved the overall risk profile of your enterprise, it's important to schedule a regular review.

Cybercrime is fast-moving and constantly developing new ways to defraud, so every business needs to keep its risk profile under review, either through a rolling programme of monitoring or a regular (possibly quarterly) revisit of the exercise you've just completed.

Each review should start from the beginning to identify newly emerging threats. It should also

include a review of the strategies that you've put in place to ensure that they are still operational and adequate to meet the evolving threat.

It is also a good idea to build this review into the business's management reporting routines. This ensures that fraud risk and fraud prevention stay front of mind for everyone from your senior leadership team through to the operatives that handle transactions and face fraud threats daily.

Keeping fraud in mind also helps to identify new risks as they emerge, allowing you to quickly tackle them before they snowball into bigger issues.



# Paypal's approach to risk and fraud management



# PayPal's approach to risk and fraud management

With over 20 years of payments experience, PayPal technology is designed to reduce the risk of fraud while boosting customers' confidence to spend.

Around the world, the PayPal brand is recognised and trusted. Customers appreciate the fact that their personal details are never shared. They can benefit from PayPal Buyer Protection and a payment experience that is designed for the easy and secure convenience today's buyers expect.

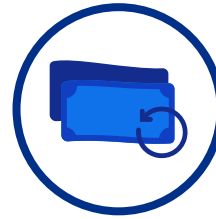
Businesses can benefit from PayPal Seller Protection and fraud prevention standards such as 3D Secure. With PayPal, sellers can offer a wide range of payment methods (including alternative payment methods) with a single integration. Additional payment methods can be switched on when required, without the need for any redevelopment or reintegration of their payment solution. That makes it easy to meet – or stay ahead of – fast-changing customer expectations without compromising security.



[PayPal](#) also offers advanced, fraud protection capabilities. Our network of 400+ million active consumers worldwide provides a rich source of data which is fed into our machine learning models for more accurate, adaptive, and real-time fraud protection capabilities; As a result, there are fewer unnecessary transaction declines and less chance of inadvertently treating your good customers like fraudsters.

[PayPal's](#) massive data set of merchants, advanced machine learning techniques and data science expertise also make it faster to identify newly trending fraudulent activity and to act accordingly across all other merchants on the network.

The results of PayPal's advanced risk management can include:



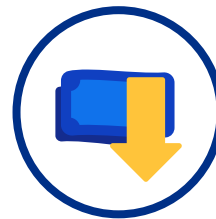
**Fewer chargebacks**



**Lower false positive rates**



**Less customer friction**



**Lower fraud losses**



**Improved operational efficiency**



**Streamlined customer experience**

Our global relationships with banks, acquirers and regulators also place us in a good position to pick up fraud before it happens.

PayPal has these risk offerings:

### **Fraud Protection**

Fraud Protection is an out-of-the-box toolkit built into the PayPal Commerce Platform, designed to help provide merchants with more visibility and control over the transaction decisioning process.

### **Fraud Protection Advanced**

Built into Braintree, Fraud Protection Advanced helps enable a merchant's fraud team(s) to identify and investigate suspicious transactions, analyse patterns, and uncover key insights to mitigate fraud losses.

Learn more about how PayPal helps enterprises to manage risk and maintain compliance [here](#).

The content of this article is provided for informational purposes only. You should always obtain independent business, tax, financial, and legal advice before making any business decision.



# References

- <sup>1</sup> Center for Strategic & International Studies (2020), [The Hidden Costs of Cybercrime](#).
- <sup>2</sup> FIS Worldpay (2021), [Global Payment Risk Mitigation](#).
- <sup>3</sup> LexisNexis (2020), [2020 True Cost of Fraud Study – E-Commerce/Retail Report](#).
- <sup>4</sup> Vesta (2021).
- <sup>5</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>6</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>7</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>8</sup> Business of Apps (2021), [Ad Fraud Statistics \(2021\)](#).
- <sup>9</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>10</sup> Aite Group, cited by Kount (2021), [What you need to know about false positives...](#)
- <sup>11</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>12</sup> Cybersource (2021), [2021 Global Fraud Report](#).
- <sup>13</sup> PayPal (2020), [How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates](#).

Thank You