pxp

Protect your business and customers

A guide to key risk factors
and best practices

Beyond Payments

A guide to help you understand key risk factors and best practices for protecting your business and your customers.

In today's digital world, securing payments is more important than ever. To help you navigate this complex landscape, we've put together this friendly guide to explain key tools and practices that ensure safer transactions for you and your customers.

3DS: Enhancing Payment Security

What is 3DS?

3D Secure (3DS) is a robust security protocol designed to protect your online payments and reduce fraudulent transactions. It adds an extra layer of verification during the payment process, helping ensure that the person making the purchase is authorized.

Why is 3DS Important?

It's one of the best tools to minimize the risk of fraud, offering both merchants and customers peace of mind.

3DS 2.0 has moved away from static passwords and now uses methods like biometric authentication and one time passcodes, improving the user experience; It has been designed to be mobile responsive, and to work with in app payments.

How Does it Work?

When a customer makes a purchase, 3DS asks for additional information (like a password or authentication code) to confirm the transaction. This helps verify the authenticity of the buyer, making it harder for fraudsters to complete unauthorized transactions.

The effectiveness of 3DS relies on the card issuer's implementation and support of the protocol. 3DS has become a widely adopted security protocol, it's not universally supported by all countries and banks.

However, in many cases, it shifts the liability for fraudulent chargebacks from the merchant to the card issuer.

Discover how PXP can enhance your business's security with 3DS.

Learn more on:

Information Hub &
Authorisation Policies

Tokenisation: Protecting Sensitive Payment Data

What is Tokenisation?

Tokenisation is the process of replacing sensitive payment data (like credit card numbers) with a unique identifier, known as a token. This token can be used in place of real card data to complete transactions without exposing sensitive details.

Why Tokenisation Matters?

Data Security
By using tokens instead of actual card numbers, you reduce the risk of data breaches.

Fraud Prevention
Even if the token is intercepted, it cannot be used for fraudulent transactions, as it's tied to a specific transaction only.

Learn more about PXP's capabilities in supporting your business with tokenisation **here**.

Chargeback Management:
Protecting Your Bottom Line

What is a Chargeback?

A chargeback happens when a customer disputes a transaction, and the bank reverses the payment. This can lead to a loss of revenue and additional fees, especially if you have a high chargeback rate.

Why Chargeback Management is Key?

Minimise Costs

Each chargeback results in lost revenue, and often, additional fees from payment processors. Effective management minimizes these losses.

Avoid Penalties

High chargeback rates can lead to account suspension and fines.

Financial Protection

Using tools like Ethoca and RDR can help you manage chargebacks efficiently, reduce fees, and protect your business.

Improving Customer Satisfaction

Effective chargeback management, especially with the use of software, streamlines the process of responding to chargebacks. This can lead to improvements in customer service, product quality, and overall customer satisfaction.

Leverage PXP's extensive expertise and comprehensive guidelines to master chargeback management best practices.

Discover more **here**.

Velocity Checks:
Preventing Fraud with Real-Time Monitoring

What are Velocity Checks?

Velocity checks monitor the speed and frequency of transactions from a specific card or account. By tracking unusual activity, these checks help identify and block fraudulent transactions in real-time.
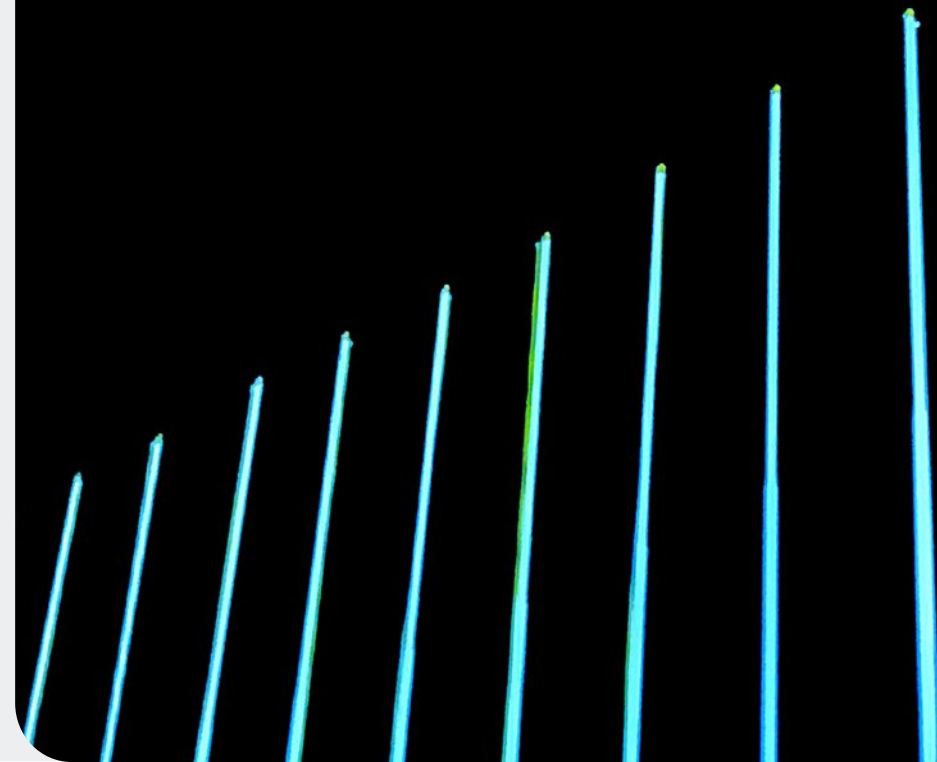
How Velocity Checks Protect You?

Prevention is Key

By identifying rapid, large-scale transactions, you can prevent fraud before it happens.

Data-Driven Decisions

Velocity checks provide useful insights into customer behaviour, helping you make smarter decisions about how to handle suspicious transactions.

Settlement Delays:
Plan ahead

Understanding the Settlement Process

Understand you cashflow to ensure you have sufficient working capital to manage any delays. Payments don't always clear instantly, settlement is the process by which your payment provider transfers funds from the customer's bank to yours.

Why It Matters

Managing this cash flow gap is key to keeping your business running smoothly, particularly if you're handling a high volume of transactions.

PCI DSS
Compliance

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to protect cardholder data. Compliance is not just a good idea—it's a requirement for merchants who process credit card transactions.

Why PCI DSS Compliance is Non-Negotiable?

Avoid Fines

Failing to comply can result in hefty fines.

Maintain Trust

Protecting your customer's payment information builds trust and safeguards your reputation.

Protect Your Business

Compliance helps avoid data breaches and costly legal consequences.

Best Practices to Protect Your Business

Clear Refund and Cancellation Policies

Make sure your refund and cancellation policies are easily accessible on your website. Clear and transparent policies help reduce the chances of chargebacks and customer disputes. A well-informed customer is a satisfied customer.

Provide Detailed Product Descriptions

To prevent disputes about "products not as described," provide clear, accurate product descriptions. The more detail you give, the less likely customers are to be disappointed, reducing the risk of chargebacks.

Efficient Dispute Resolution

Having a clear process in place to handle customer disputes ensures that any issues are resolved quickly and fairly. This can prevent issues from escalating into chargebacks or other negative consequences.

Record Keeping for Disputes

Keeping thorough documentation can be invaluable when responding to disputes or chargebacks. This will also serve as proof that your business operated within the guidelines of best practices.

Multi-Factor Authentication and OTP Verification

Add an extra layer of security by using Multi-Factor Authentication (MFA) for account logins and One-Time Passwords (OTPs) to verify transactions. This helps ensure only legitimate users access accounts and that payments are authorized by the cardholder.

CAPTCHA & Bot Protection

Prevent automated attacks and bot-related fraud by integrating CAPTCHA challenges at critical points like logins and checkouts. This will help protect your site from malicious automated attacks.

Contact Us

For more information, **contact us** or reach out to your Account Manager directly.