A NetPay guide to...

Understanding the Jargon and Acronyms

Understanding the Jargon and Acronyms

3-D Secure

3-D Secure is a protocol designed to be an additional security layer for online credit and debit card transactions. It was developed by Visa and MasterCard with the intention of improving the security of Internet payments and is offered to customers under the name **Verified by Visa**. Services based on the protocol have also been adopted by MasterCard as **MasterCard SecureCode**, and by JCB International as **J/Secure**. Also American Express added it, as **SafeKey**.

When online payments are not performed using 3D Secure they are considered to be 'non-secure'

transactions. Non-secure transactions attract a higher premium than standard online transactions because it has not been possible to provide the same level of verification of the cardholder as is possible with 3D Secure.

This charge typically is an increase % for credit card transactions and an additional charge in pence for debit cards. NetPay always recommends that online transactions use 3-D Secure, providing an additional layer of security and keeping transaction costs to a minimum.

Acquiring Banks (Acquirer)

An acquiring financial institution is a bank that processes and settles a merchant's daily debit/credit card transactions as well as providing the relevant share of the transaction charges levied to the merchant to the card issuer and the scheme the card is operated under. Merchants must maintain such an account to be able to accept payments by debit and credit card. Daily card transaction totals are deposited in the merchant's account after settlement. In this way, such a financial institution acquires, or serves as the intermediary, to facilitate the transaction and pays the merchant the funds it has acquired on its behalf.

Examples of acquiring banks:

- **Streamline** – NatWest, RBS, Ulster Bank, NetPay & Independents.
- **Barclaycard Merchant Services (BML)** – Barclays & Independents.
- **Elavon Merchant Services** – Santander & Independents.
- **First Data** - Lloyds TSB, Bank of Scotland, Allied Irish Bank, Halifax, Independents
- **Global Payments Inc.** – HSBC & Independents

NetPay uses Streamline as its acquiring bank.

AML - Anti Money Laundering

Money Laundering is the process whereby criminals attempt to conceal the true origin of the financial proceeds of crime. The Money Laundering Regulations require internal controls, policies and procedures to combat money laundering.

API - Application Programming Interface

An API specifies how software components should interact with each other. A practical example would be an API (written by our developers) to enable e-commerce integration of the NetPay online payments capability into the majority of e-carts used on the web today. (See Shopping Cart)

Bluetooth

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength radio transmissions from fixed and mobile devices, creating personal area networks with high levels of security. An example would be a NetPay Bluetooth terminal connected to its base station; the base station would then be connected to a phone line or broadband as required. The device would communicate using Bluetooth with its base station which would then use the connectivity from that base station to communicate with the acquiring bank for authorisation.

BRAM - Business Risk Assessment & Mitigation

The BRAM program is operated by MasterCard and among other things, prohibits a merchant from submitting for payment, and an acquirer from accepting from a merchant for submission for payment to the Scheme network any transaction that is fraudulent, illegal, or is deemed to damage or have the potential to damage the goodwill of the MasterCard brand. The following activities are prohibited under the BRAM program:

The sale or offer of sale of a product or service other than in full compliance with all laws applicable to the Acquirer, Issuer, Merchant, Cardholder, Cards.

Card Scheme

Owners of a payment scheme, into which a bank or any other financial institution can become a member. By becoming a member of the scheme the member then gets the possibility to issue or acquire the transactions performed within the scheme.

Examples are: **Visa, MasterCard, American Express, Diners Club, JCB, and Maestro.**

Understanding the Jargon and Acronyms

CAT - Cardholder Activated Terminal & UPT - Unattended Payment Terminal

A remote device that reads captures and transmits Card information in an Unattended Environment that is without the presence of a merchant representative. Types of terminals include ATMs, Automated Fuel Dispensers and Ticket Dispensing Machines.

Contactless

A payment terminal which is configured to accept contactless card payments.

In the case of the NetPay Ingenico manufactured terminals, to process a contactless card transaction you simply get the consumer to place their contactless card in-front of the terminal screen, after you have input the sales value and pressed the green button. Not all terminal manufacturers and devices support contactless.

The transaction must be less than £20 (including any tips) and cannot include cashback. You also cannot refund contactlessly. On the 3rd contactless transaction within a 24 hour period even if the card is presented a PIN number will still be required to be input, this is to reduce the risk of contactless fraud.

CBA - Cross Border Acquiring

Cross-border acquirers are banks or organisations that enable you to accept cards in up to 34 European countries - with a single contract.

If your business operates in more than one European country, you can avoid the complexity and expense of setting up contracts with acquiring banks for each country by choosing a cross-border acquirer.

The benefits of cross-border acquiring are:

- **Streamlined operations:** This type of centralised acquiring means there is no need for separate terms of business, separate settlement periods and complicated behind-the-scenes reconciliation. It streamlines your operations and saves you administrative costs.

No merchant is permitted to operate their services in other countries without a cross border acquiring agreement in place.

Chargebacks

Normally where a cardholder raises a chargeback via their card issuer, typically for goods or services not provided, quality of goods or service disputed, warranty claims. The cardholder will always be encouraged to resolve the issue with the merchant in the first instance with a chargeback always being considered a last resort.

A merchant will be charged a fee by the acquirer for every chargeback (irrelevant if justified or not) to cover the administration of issuing the chargeback and refunding the monies to the merchant
(if required). (See also MPL)

CNP - Card not Present

Card Not Present (CNP) transactions occur where there is no card or cardholder present, i.e. orders via mail, telephone, fax as well as Internet/eCommerce payments. In order to process these transactions
it is likely you will need a supplementary agreement.

Although, this option provides you and your customers with a flexible payment method, taking transactions of this type does mean that you are more at risk of fraud because you do not come into contact with the card or cardholder, these transactions are likely to incur a premium charge
as a result of this. (See also 3-D Secure)

CHP - Cardholder Present

These are face-to-face transactions where your customer and their card are with you at the point
of sale.

Chip and PIN is the usual way to accept card payments on your terminal when the card and cardholder are present as well as contactless. Some customers, however, will continue to sign to authorise payments and this could be due to an impairment that prevents them from inputting their PIN. Some cardholders will still have magnetic stripe only cards and these must not be refused at the point of sale. It is worth noting that the many International cards do not include Chips, in particular cards from the USA where only the magnetic stripe is available.

CDD - Customer Due Diligence

CDD in the financial sense describes the process by which a bank or financial institution checks the identity, background and other aspects of the source of wealth of potential and existing customers.

Legislation and regulation require NetPay to obtain evidence of identity of a customer at recruitment and to keep a record of that evidence for as long as there is a relationship with a customer.

Understanding the Jargon and Acronyms

CV2 - Card Verification Value

All credit and debit cards carry a security code number. This number is known to the bank and printed on the card, but is not stored or printed anywhere else. Therefore, it can be used as a check that when you make your purchase you are in physical possession of the card, or have at least seen the card at some time. On most cards, the security code number is the last three digits of the number printed on the back, at the top right of the signature strip (in the case of American Express it is 4 digits). You will be required to enter this additional security number for "card not present" payment card transactions against credit card fraud before your transaction can be completed.

A card security code (CSC), sometimes called card verification data (CVD), card verification number (CVN), card verification value (CVV or CVV2), card verification value code (CVVC), card verification code (CVC or CVC2), verification code (V-code or V code), card code verification (CCV), or signature panel code (SPC) are other acronyms for this security feature.

DSS - Data Security Standards

(See PCI DSS)

EPOS - Electronic Point of Sale

An electronic method of retail checkout, usually self-contained. The system involved is typically capable of all tasks of a store checkout counter: payments by bank or credit cards, transactions verification, sales reporting, inventory data updates. It also facilitates customer service and inventory availability.

EMV - Europay, MasterCard & Visa

A global standard for inter-operation of chip payment cards, chip card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

FCA - FCA Financial Conduct Authority - previously known as the FSA

The FCA regulates the financial services industry in the UK. Their aim is to protect consumers, ensure the industry remains stable and promote healthy competition between financial services providers.

FSA - Financial Services Authority

Renamed Financial Conduct Authority (FCA)

GBPP - Global Brand Protection Programme

The GBPP is a Visa operated program (similar to the BRAM program operated by MasterCard) to prevent merchants from processing illegal or unethical credit card transactions, such as: illegal prescription drug sales, deceptive marketing, and incorrect coding of online gambling transactions, use of fraudulent websites that solicit donations or pose as official government sites. Introduced as a result of increased fraud associated with card not present (CNP) transactions.

GPRS - General Packet Radio Service

GPRS is a packet oriented mobile data service on the 2G and 3G cellular communication system's global network for mobile communications. An example would be a NetPay GPRS terminal fitted with a global sim enabling you to connect to the provider networks with the strongest mobile signal available. Once that connection is made you are able to process your card payments anywhere a mobile signal is available.

GUI - Graphical User Interface

A GUI is a type of user interface that allows users to interact with electronic devices through graphical icons and visual indicators. Examples of GUI's most familiar to people today would be Microsoft Windows or Mac OS for desktop and laptops. Blackberry OS, Android & Apple iOS for handheld devices (smartphones).

Hosted Form

A solution which enables a customer to go through the purchasing process on a merchants website, when the payment stage is reached they are passed to the payment service provider gateway via (HTTPS see below) where the customer inputs their credit/debit card information and submits the transaction for processing. This method enables you to accept credit/debit card payments quickly and easily with very little integration, but also importantly without having to handle or store card information and as a consequence relaxes PCI DSS compliance obligations surrounding the storage of card information. (See also 3-D Secure, PCI DSS, and PSP - Payment Service Providers)

Understanding the Jargon and Acronyms

HTTPS - Hypertext Transfer Protocol

HTTPS is a communications protocol for secure transmission over a computer network. Historically, HTTPS connections were primarily used for payment transactions on the Internet, e-mail and for sensitive transactions in corporate information systems. In the late 2000s and early 2010s, HTTPS began to see widespread use for protecting page authenticity on all types of websites, securing accounts and keeping user communications, identity and web browsing private.

Ingenico

Is a worldwide company, whose business is to provide the technology involved in secure electronic transactions. Its traditional business is based around the manufacture of point of sale payment terminals, but it now also includes complete payment solutions and related services.

NetPay supply Ingenico terminals to its merchants.

Interchange Fees

Interchange fee is a term used in the payment card industry to describe a fee paid between banks for the acceptance of card based transactions. Usually it is a fee that a merchant's bank (the "acquiring bank") pays a customer's bank (the "issuing bank").

For credit cards, the fee is generally a small percentage of the value of the transaction; for debit cards, it is usually a small flat fee. Interchange fee levels also vary depending on the type of card, its associated risk, and the country where the transaction takes place.

These fees are set by the issuing banks.

ISO - Independent Sales Organisation

An ISO or Managed Service Provider (MSP) sells merchant services from an acquiring bank to merchants, directly via wholesale or indirectly via a variety of sales channels.

There are a number of ISO's in the UK. NetPay is an ISO.

Magstripe - Magnetic Stripe

Data encoded in the magnetic stripe of a card, used for authorisation during CHP transactions.

There are three tracks on the magnetic stripe. Each track is about one-tenth of an inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 6-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 4-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 4-bit plus parity bit characters.

Your credit card typically uses only tracks one and two. Track three is a read/write track (which includes an encrypted PIN, country code, currency units and amount authorised), but its usage is not standardised among banks.

The information on track one is contained in two formats: A, which is reserved for proprietary use of the card issuer, and B, which includes the following:

- **Start sentinel** - one character
- **Format code="B"** - one character (alpha only)
- **Primary account number** - up to 19 characters
- **Separator** - one character
- **Country code** - three characters
- **Name** - two to 26 characters
- **Separator** - one character
- **Expiration date or separator** - four characters or one character
- **Discretionary data** - enough characters to fill out maximum record length (79 characters total)
- **End sentinel** - one character
- **Longitudinal redundancy check (LRC)** - one character LRC is a form of computed check character.
- The format for track two, developed by the banking industry, is as follows:
- **Start sentinel** - one character
- **Primary account number** - up to 19 characters
- **Separator** - one character
- **Country code** - three characters
- **Expiration date or separator** - four characters or one character
- **Discretionary data** - enough characters to fill out maximum record length (40 characters total)
- **LRC** - one character

Understanding the Jargon and Acronyms

MMSC - Minimum Monthly Service Charge

Acquirers and ISO's commonly impose what is known as a minimum monthly service charge. This is effectively the minimum amount they require each month to maintain the acquisition service/merchant account. If the total cost of transaction processing to the merchant exceeds the minimum charge required then no additional charge will be levied, if it is less a balancing charge will be made.

MOTO - Mail Order / Telephone Order

MOTO transactions are performed over the internet by using a "virtual" terminal with the card holder either being on the end of the phone or having submitted their credit/debit card details via a mail order. A "virtual" terminal is effectively a secure payment screen within a web browser that enables the merchant to input the various personal details of the consumer/card details and passing them to the payment service provider's gateway for processing.

NetPay have segmented their Revolution and MOTO portals to ensure that those responsible for taking payments only do not have visibility of the broader capability Revolution provides.

MID - Merchant Identification

A merchant ID allows your business to be identified by the banks and credit card institutions, in order to accept credit card payments on behalf of your business, regardless of which type of services or products you are offering. Traditionally, in order to be given permission to accept credit card payments, you needed to be granted merchant status strictly through the acquiring bank itself, but independent sales organisations (ISOs) can help you obtain a merchant ID as well.

MSP - Managed Service Provider

(See ISO)

MCC - Merchant Category Code

MCC is a 4 digit number assigned to a business type by an acquirer.

It is very important that the merchant category code is correct and reflects the type of business which the merchant is engaged in. This would be determined at the point of signing a prospective merchant. Failure to define the correct category may expose us to card scheme fines, the creation of chargeback rights, affect MPL calculations and authorisations.

(See Sector Policy Risk & MPL)

MRP - Maestro Recurring Payments

The ability to make recurring payments via a Maestro card is no longer support under new card scheme rules.

MPL - Merchant Potential Liability

Merchant acquiring creates a contingent liability for the acquiring bank which is referred to as Merchant Potential Liability (MPL). A contingent liability is where a financial exposure arises from entering into an acquiring relationship with a merchant; however this only results in debt to the acquirer in the event of the merchant ceasing to trade and refunds being due to the card holder for the non-delivery of goods or services.

This accumulated debt from merchant failure is accrued through cardholders raising chargebacks via their card issuer.

(See also Chargebacks)

MPL Quantification

Quantification is achieved using a formula made up of:

- Card turnover processed or projected per annum.
- Specific Merchant Fulfilment Period for goods/services provided by the merchant
- Credit Conversion Factor for the merchants Category Code based on our past experience

The formula is therefore;

- Card turnover (£) x SMFP (days) divided by 365 (days) x Credit Conversion Factor (%) = MPL (£)

Understanding the Jargon and Acronyms

PAN - Primary Account Number

The primary account number is the credit/debit card number that identifies the issuer and the particular cardholder account.

The first digit in your credit card number signifies the system, **(Major Industry Identifier MII)**:

1 & 2. Airlines

3. Travel/entertainment cards and banking/financial

4. Banking/financial

5. Banking/financial

6. Merchandising and banking/financial

7. Petroleum

8. Healthcare

9. National assignment

Amex, Diners Club and JCB are in the travel and entertainment category.

Visa & MasterCard are in the banking/financial category.

Shell Oil and BP are in the petroleum category.

The Issuer Identification Number (IIN) is the first 6 digits of a card number (including the MII digit).

These identify the institution that issued the card. The rest of the number is allocated by the issuer.

PEP - Politically Exposed Person

A PEP can be defined as an individual who is or has been entrusted with a prominent public function; examples include heads of state, senior politicians, government, judicial or military officials, senior executives of state owned corporations and political party officials. They may be considered High Risk as their position and influence may enable such individuals to illegally derive personal gain.

PCI DSS - Payment Card Industry Data Security Standards

(PCI DSS) is a proprietary information security standard for organisations that handle cardholder information for the major debit, credit, prepaid, ATM, and POS cards.

Defined by the Payment Card Industry Security Standards Council, the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure. Validation of compliance is done annually — by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organisations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

There are 4 levels of compliance:

- **Level 1:** Any merchant processing over 6M Visa or MasterCard transactions per year, or identified by a card scheme as a Level 1 merchant and any merchant compromised in the last year.
- **Level 2:** Any merchant processing 1M to 6M Visa or MasterCard transactions per year.
- **Level 3:** Any merchant processing 20,000 to 1M Visa or MasterCard e-commerce transactions per year.
- **Level 4:** Any merchant processing fewer than 20,000 Visa or MasterCard e-commerce transactions per year, and all other merchants processing up to 1M Visa or MasterCard transactions per year.

PWCB - Purchase with Cash Back.

The facility enabled by the acquirer for the merchant that allows the cardholder to request cash at the point of sale up to the value of £100.

Authorisation is required. This must be enabled as part of the merchants agreement with the acquirer.

Pre-Auth

Advance approval of funds and validity of the card. Pre-auth does not physically debit the card but ring fences the funds on the card holder's card preventing it from to be spent with another merchant. Pre-auth is only available to Car Hire and Hotels businesses only.

PSP - Payment Service Providers

An organisation that provides a secure payment route/gateway from the merchants website/online shopping carts to their chosen acquiring bank. A PSP will also typically provide other software features that enable payments to be taken through the web or via an API.

NetPay is a Payment Service Provider

QSA - Qualified Security Advisor

(See PCI DSS)

Refund

The process whereby a credit is applied to a cardholders account. Should NOT be authorised (as will increase cardholder available funds).

Understanding the Jargon and Acronyms

Revolution

Revolution is the name of the NetPay's market leading and feature rich portal that has no equal in the merchant services market today. It is a web based system that allows you to manage your services with NetPay and see detailed performance reporting and analytics. The platform is multi-channel; this means you can have consolidated visibility of both your online and terminal based transactions from one platform improving visibility of business performance

Reversal (Implicit)

A reversal transaction issued by the acquiring bank, if no response is received from the merchants host the process cancels the authorise request. This may happen when an initial request to process a card is initiated but before the authorised response is received by a terminal device it loses connectivity or has an issue which causes it to reboot.

Reversal (Explicit)

A reversal transaction issued by a merchant to cancel the previous transaction.

To be able to initiate a reversal it must be the next transaction on the same terminal ID, if a separate transaction takes place after the transaction that is required to be reversed then a reversal cannot take place and a refund must be issued.

Recurring Transaction

A transaction that occurs on a regular basis. (Magazine subscription being one example). NetPay provide a service called SchedulePay that supports the ability to take payments on a recurring basis (see SchedulePay).

ROC - Report on Compliance

(See PCI DSS)

SAQ - Self Assessment Questionnaire

(See PCI DSS)

Sector Policy Risk

There are 4 categories that a type of business can operate under:

- **General** – Merchant can be recruited by any sales channel.
- **Restricted** – Merchant visit must happen, and ensure compliance to the appropriate sector policy.
- **Refer** – As restricted plus additional approval required.
- **Prohibited** – Merchant must not be recruited under any circumstances.

Sector policy risk operates to ensure that credit risks for new and existing merchants acquired in various sectors are assessed and approved in a consistent manner taking in to account the key risk drivers.

Sector policies relating to trading sectors currently include:

Airlines, Leisure, Merchant Aggregators, Gaming and Gambling, Hotels, Travel, Insurance, Money Service Businesses, Adult.

Within each of the above, the appetite is split in to 3 categories:

- **Positive** – The prime focus for new business
- **Cautious** – Areas where new business can be taken on, but on a more selective basis.
- **Negative** – Only exceptional cases will be considered, otherwise not approached.

(See also MCC and MPL)

SchedulePay

SchedulePay is an application developed by customers and provides the ability for merchants to setup recurring credit and debit card transactions with card holders, processing payments weekly, monthly, quarterly or annually.

SchedulePay agreements will continue until they are cancelled, the card expires or the payment fails.

NetPay offers SchedulePay as part of its merchant services.

Understanding the Jargon and Acronyms

Shopping Cart (Software)

also known as **e-commerce software**

A shopping cart is a piece of e-commerce software on a web server that allows visitors to an Internet site to select items for eventual purchase. Upon checkout, the software typically calculates a total for the order, including postage and packing charges and the associated taxes, as applicable.

(See Hosted Form to understand the payment stage). This shopping cart will integrate with a PSP like NetPay to support the debiting of the payment for those goods or services at the end of the purchasing process.

Some of the top shopping carts include: **Agora, CS-Cart, Magento, nopCommerce, Opencart, osCommerce, Prestashop, WooCommerce, Zen Cart, Zeus Cart.**

NetPay have an XML API which integrates with these shopping carts.

SMFP - Specific Merchant Fulfilment Period

The length of time (days) a merchants business takes to fulfil goods or services to the card holder. The longer the period for fulfilment the higher the risk the business is considered to be.

(See also MPL)

TPPA - Third Party Payments Aggregation

Third party payments aggregation (TPPA) is a description used for merchants that are selling a product or service that they do not own. The best example of a TPPA (aggregator) is **PayPal**. They simply facilitate the exchange of money between two parties.

There are, however, different types of TPPA's. For example, an online air travel booking site may charge both their service fee and the actual airfare in a single transaction. If the merchant were only charging their service fee, they would not fall into the TPPA category as they are simply charging for the service they provide but if they are also charging a credit card for a product they do not own, an airfare ticket in this example, they fall into the TPPA category.

Because the card acquirers and schemes have discouraged the practice of TPPA and the increased risk, most merchant account providers are justifiably reluctant to underwrite these types of accounts.

Tokenisation

Tokenisation is the process of replacing sensitive data with unique identification symbols. It enables merchants to send card information and receive a 'token' back that they can use for any subsequent transactions with that card but importantly prevents them from having to store the card number locally increasing the merchant's obligations under PCI DSS compliance. Tokenisation has become a popular way for businesses to bolster the security of credit card and e-commerce transactions whilst relaxing certain obligations under PCI DSS compliance.

NetPay offers Tokenisation as part of its online/eCommerce value added services.

TID - Terminal Identification

Terminal Identification Number, also known as a TID, is a unique number assigned and linked to a specific terminal (be it physical or virtual) which is used to identify the merchant operating the terminal during the card sales transaction processing. This number is also required to set up online processing through payment gateways with a TID required for each concurrent transaction. It is provided by the payment service provider with which a company has established their online payment service with or allocated by the manufacturer of the terminal hardware that is being supplied as part of the service. The number not only identifies which company is using what specific terminal, but also tracks each POS transaction made at that specific location. Typically, the number is seven digits long not including any leading zeroes.

"Virtual" terminal

(See MOTO)

XML API - Extensible Markup Language Application Programming Interfaces

XML is a markup language that defines a set of rules for encoding documents in a format that is both human & machine readable. API's have been developed to assist software developers with processing XML data and creating a deeper integration with applications to provide a more seamless experience to their user.

NetPay Merchant Services

UK

T +44 (0)333 311 0200
E getintouch@netpay.co.uk
W www.netpay.co.uk