worldpay
from FIS

WELCOME TO WORLDPAY FROM FIS

Give yourself every advantage.

Let's get started

Welcome to Worldpay from FIS and thank you for your business! The Worldpay team understands that your job is to run your business, not to worry about payment processing. That is why we created Worldpay with one goal in mind: To help businesses like yours capture every sale with easy-to-use, reliable payment processing solutions that provide unparalleled security for you and your customers.

Designed to make your business mighty powerful

As a member of Worldpay, you now have access to business-building products and services, payments tools and resources, a dedicated and reliable support team 24x7x365 and more – all through a program designed to help you make the most out of your investment in payments. Start enjoying your exclusive benefits today.

We understand that the most important part of our relationship happens after you sign a processing agreement with us. So on behalf of the entire Worldpay team, welcome and we look forward to a long-lasting relationship that exceeds your expectations.

Warmly,

The Team at Worldpay from FIS

The advantage is yours.

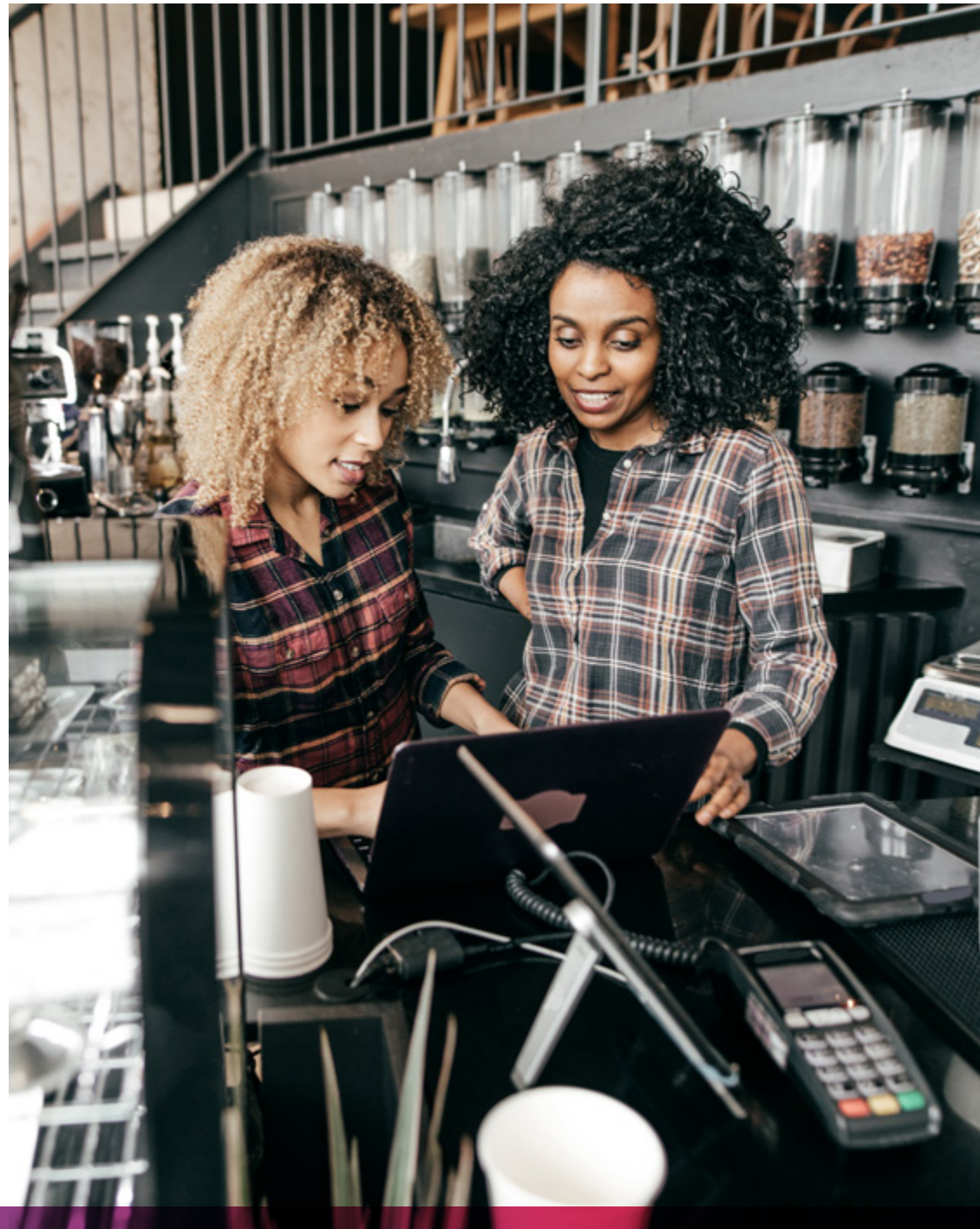
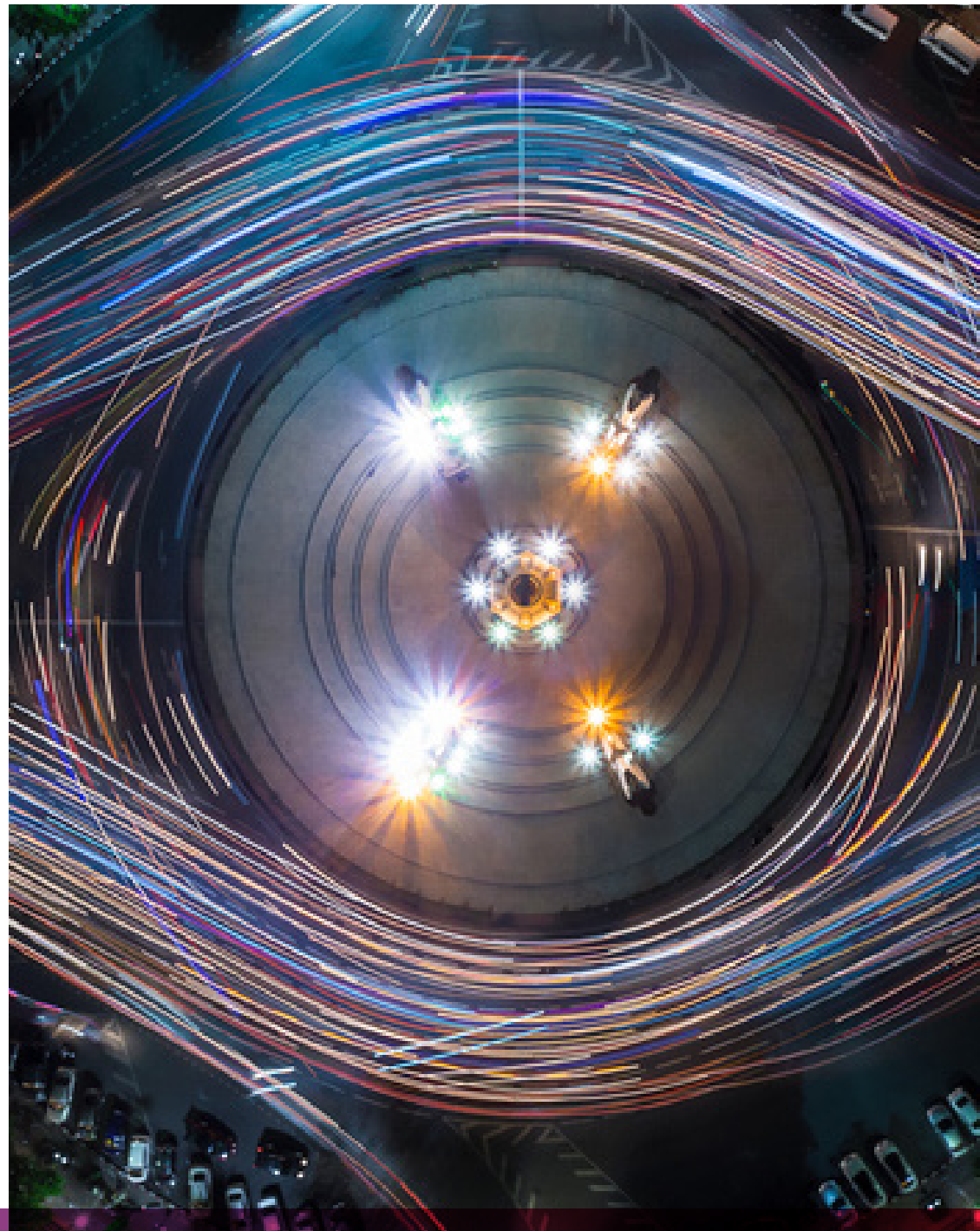


Table of contents



Payment Card Industry - Data Security Standards (PCI DSS) overview

What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS), is a set of security standards that were created by the major credit card companies (American Express, Discover Financial Services, JCB, Mastercard Worldwide, and Visa International), to protect their customers from identity theft and security breaches. Under the PCI DSS, a business or organization should be able to assure their customers that its credit card data/account information and transaction information is safe from hackers or any malicious system intrusion. There are 12 key requirements to achieving PCI DSS compliance:

Build and maintain a secure network

Requirement 1. Install and maintain a firewall configuration to protect cardholder data.

Requirement 2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect cardholder data

Requirement 3. Protect stored cardholder data

Requirement 4. Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

Requirement 5. Use and regularly update anti-virus software

Requirement 6. Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7. Restrict access to cardholder data by business need-to-know

Requirement 8. Assign a unique ID to each person with computer access

Requirement 9. Restrict physical access to cardholder data

Regularly monitor and test networks

Requirement 10. Track and monitor all access to network resources and cardholder data

Requirement 11. Regularly test security systems and processes

Maintain an information security policy

Requirement 12. Maintain a policy that addresses information security

The first version of PCI DSS was introduced in September 2006. At this time, the PCI Security Standards Council established a continual two year cycle of review and revision of PCI DSS. For the most current information regarding PCI DSS, visit www.pcisecuritystandards.org.

Peace-of-mind PCI DSS compliant payment processing solutions

Worldpay is committed to providing you with solutions that meet or exceed the requirements of PCI DSS. To learn more about PCI DSS visit Worldpay's website at Worldpay.com or the PCI Security Standards Council Website at www.pcisecuritystandards.org.

Merchant point of sale - Guidelines

Face-to-Face Transactions—Check All Card Security Features

Check the card for a hologram

A hologram is a three-dimensional symbol in either gold or silver foil that is designed to help deter counterfeiting. The image should reflect light and appear to move when you tilt the card. The Visa hologram is a dove. The Mastercard hologram is two interlocking globes.

Check the expiration date

The card is valid through the last date of the month. Do not accept an expired card.

Check the valid date

Some cards will have this feature, in which the card is not valid until the date shown. Do not accept an invalid card.

Check the four digits

For Visa and Mastercard cards, the first four digits of the embossed card number must match the four digits pre-printed above or below that number.

Check the draft for a clear impression when using a manual imprinter

This will ensure that you have captured the embossed card account number. Complete the draft with the date, description of merchandise/service, sales tax, total dollar amount, authorization number and signature.

Obtain a manual imprint of the customer's card. When using an electronic printer and the card can not be magnetic-strip read

Obtaining a manual imprint of the card will ensure that you have captured the embossed card number. Use the manual sales draft to complete the transaction.

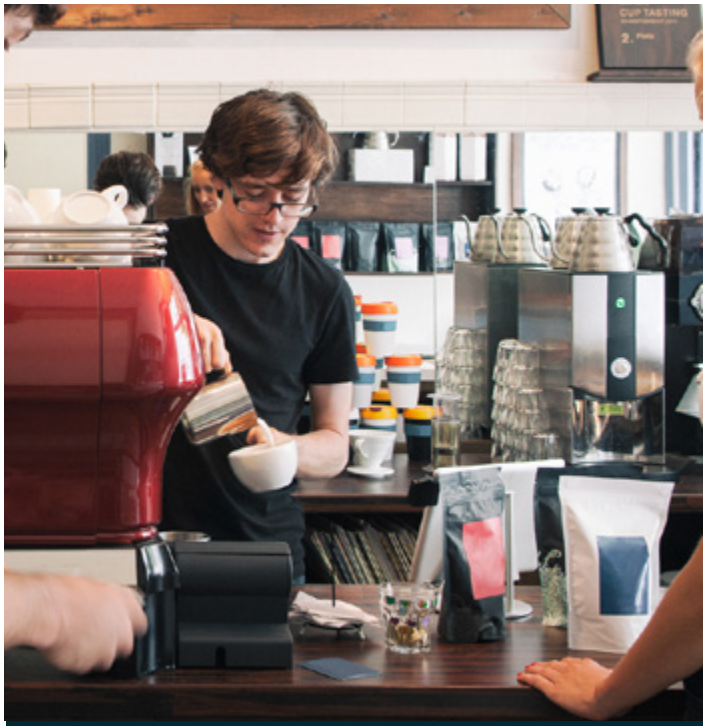
Obtain the customer's signature

Match the signature on the draft to the signature on the back of the card.

If the customer's card is unsigned, request another form of identification with a photo and signature. Request that the customer sign his or her card and then compare the signatures. If the customer refuses to sign, inform him that you are unable to accept an unsigned card for payment and request another form of payment.

Storage of drafts

Merchants must store all paper copies of sales drafts for 18 months—whether you process manual drafts or electronic receipts. This ensures that you can produce copies of requested drafts and avoid being charged back for non-receipt of requested item. Store your drafts in their original batches, in date order, for easy location. Mail and telephone order merchants may benefit from facsimile drafts, from which we can produce a facsimile of sales receipt for mail and telephone orders using information originally provided in settlement. Contact your customer service representative for more information on this service.



Remember:

Hold the card until the transaction is completed! Retaining the card throughout the transaction enables you to complete all of the security checks without having to ask the customer to re-present his or her card for a signature comparison or possible "call center" procedure. You will avoid check-out delays and ensure a smooth transaction.

What to look for - Face-to-face transactions

Look for physical evidence

- The hologram is missing or of poor quality
- The customer's signature does not match the one on the card
- A Mastercard signature panel does not contain the Mastercard wordmark
- A Visa card signature panel does not contain the titled Visa pattern
- The card is warped or has a dull finish
- The account number and cardholder name are ironed out and the card is embossed with a different number—evidence of this alteration is noticeable on the back of the card
- The account number is titled or slanted, or the embossed data spacing is off
- The printed information is on top of the laminated surface of the card
- The printing on the back of the card is blurry or distorted
- Information displayed on the terminal or electronic printer receipt does not match the account number embossed on the front of the card

Be alert for suspicious behavior

- The customer appears nervous or overly talkative
- The customer buys clothing without trying it on for size
- The customer questions the sales clerk about the floor limit, and then makes several separate purchases that approach but do not exceed the floor limit
- The customer declines the alterations or delivery although they are included in the price
- The card is produced from a pocket, not a wallet
- The customer signs the sales draft in a deliberate or unnatural manner
- The customer presents only a temporary driver's license without a photo

Card-not-present transactions
How to reduce your risk of fraud

In the mail and telephone order business, payment by card is the preferred method—unfortunately it can be a risky one. When neither the card nor the customer is physically present at the point of sale, the merchant experiences the greatest exposure to disputes, chargebacks and fraud. Guidelines have been developed to help reduce this exposure for mail and telephone order sales.

Authorize every sale on the order date

Authorizations are valid for a specific number of days: Visa—up to 7 days, Mastercard—up to 30 days.

Merchandise must be shipped and sales must be deposited within these timeframes or the authorization will expire. If your shipping date exceeds these timeframes, obtain a new authorization code before shipping the merchandise.

Remember:

For retail or face-to-face sales, the card and the cardholder must be present at the point of sale. All sales in which the card is not present either in person, by mail or by telephone order, are taken at your own risk. However, reviewing the following guidelines may help you make more informed decisions on whether to accept such sales at your business.

What to look for - Face-to-face transactions (continued)

Record the card account number

A Visa card number begins with a 4 and has 13 or 16 digits.
A Mastercard card number begins with a 5 and has 16 digits.

Ask for both a billing and shipping address

If the addresses differ, determine whether the difference seems reasonable.

Ask for the customer's phone number

Ask for the phone number not as a condition for accepting the sale, but as a customer service tool. This enables you to call the customer for various reasons: to inform him or her that merchandise is back ordered, to request another form of payment if the authorization is declined or to verify information if the caller seems unclear about address details.

Ask for the code on the back of the card Visa Card Verification Value 2 (CVV2) or Mastercard Card Validation Code 2 (CVC2)

Turn the card over and read the last three digits, which trail the account number printed in the signature panel (this is the CVV2 or CVC2 code).

Note: Merchants who request the CVV2 or CVC2 code will receive a match or no match response when entering the transaction into a terminal for processing.

Use the Address Verification Service (AVS)

AVS enables you to compare the billing address provided by the customer with the billing address on file at his card-issuing bank. You receive a verification code indicating a match or partial match. While this is not a guarantee against chargebacks, it allows you to make more informed decisions before shipping. Contact your customer service representative for more information on utilizing AVS.

Do not deposit sales until the ship date

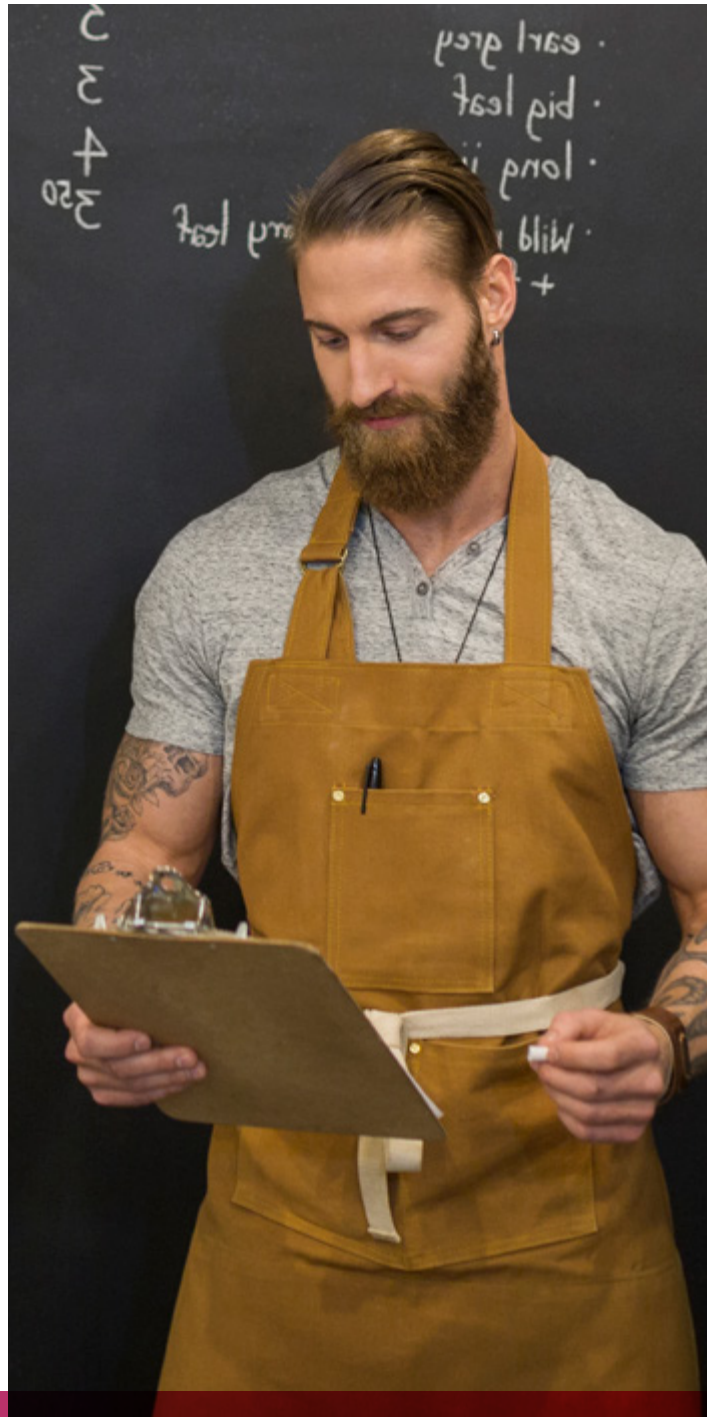
Visa and Mastercard regulations do not permit merchants to receive payment for sales until the goods or services are delivered to the customer. Obtain an authorization on the order date, but do not deposit the sale until the ship date. Visa transactions for custom-ordered merchandise may be deposited on or after the order date, under the condition that the merchant has informed the customer that he will be billed prior to shipping.

Mail an order confirmation notice to the cardholder prior to shipping

This will not prevent chargebacks, but may reduce the number of inquiries and ticket requests.

Request that your customer service number appears on the customer's credit card statement

Both Visa and Mastercard regulations permit mail and telephone order merchants to place their customer service telephone number where the merchant city would normally appear. This may help the customer recognize the charge when it appears on the statement and reduce the number of ticket requests and disputes. Contact your customer service representative to discuss this option.



Top ten warning signs - Fraudulent telephone and mail order transactions

1. Hesitant caller

Beware of callers with shaky voices or delayed responses to questions. This may indicate that the caller is not comfortable with the information.

2. Rush orders

Rush orders are a favorite weapon of the “here today/gone tomorrow” schemes.

3. P.O. boxes and mail receiving services

Most delivery services will not deliver to these addresses. This may indicate lack of permanent address.

4. Above-average transaction amounts

Merchants often know the amount of an average sale. Be wary of those transactions that greatly exceed the norm.

5. Purchases that can be easily converted to cash

Examples include electronics, jewelry and leather goods.

6. Geographic location

The top five states with fraudulent activity are California, Florida, Illinois, New York and Texas.

7. 1-800 return phone numbers

Be suspicious of toll-free telephone numbers when given as the day or evening phone number. Attempt to get a direct line instead.

8. Multiple orders in a short period of time

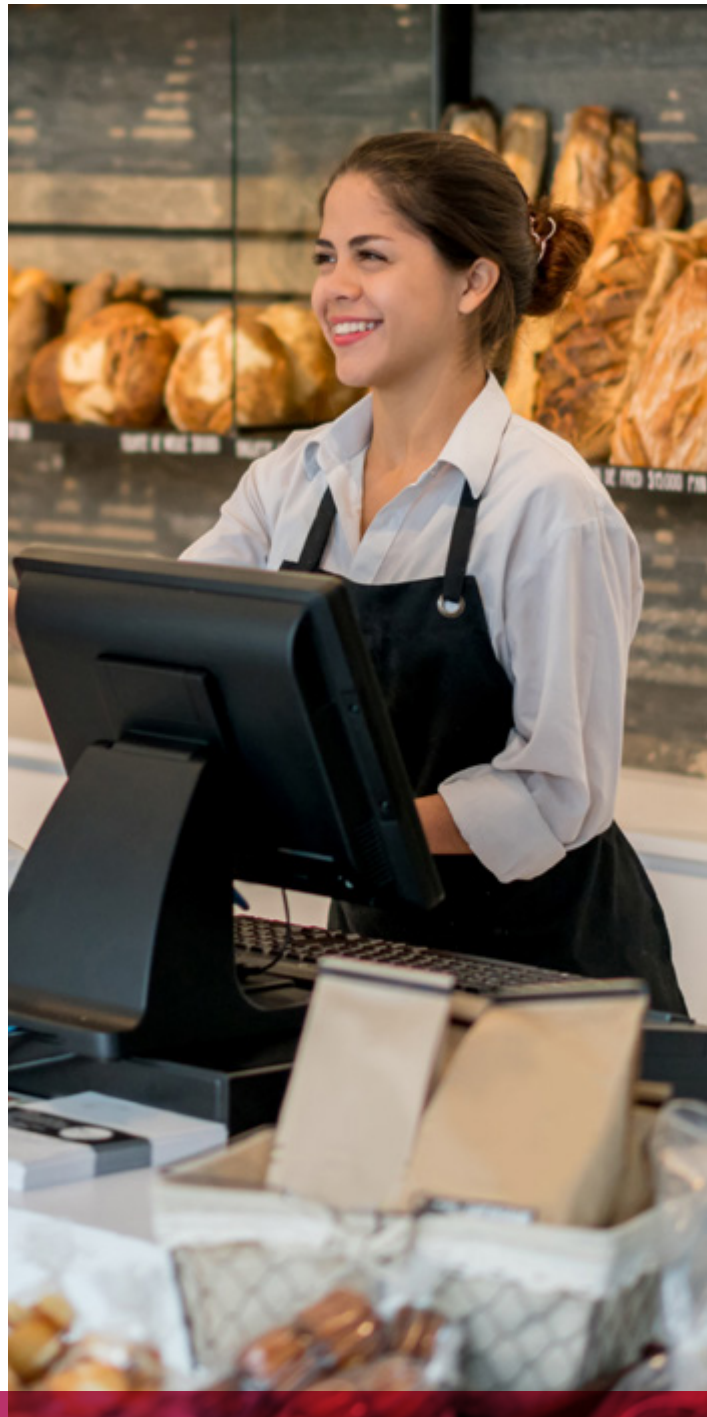
Many merchant systems show all orders placed to a certain account or unique customer number. Be especially aware of multiple orders.

9. Unusual transaction sequences

If the customer typically purchases only accessories and novelty items, but calls in to purchase a new spring wardrobe there may be cause for verification.

10. Fourth quarter

Fraud is always a consideration, but fraudulent activity seems widespread, particularly around the holidays.



eCommerce Transactions - Signs of potential fraud

Processing electronic commerce transactions
Be alert for the following:

- A first purchase which is also typically the sole purchase made, allowing criminals to minimize the possibility of identification associated with recurring purchases
- Larger than normal orders that maximize purchases on time-limited stolen or bogus payment card accounts
- Orders consisting of multiples of the same item or big-ticket items that maximize resale value and profit potential
- Orders shipped rush or overnight to deliver fraudulently obtained items as soon as possible for quick resale
- Orders from Internet addresses using free e-mail services that do not require a billing relationship or verification that an account was opened by a legitimate cardholder

eCommerce data security
Best practices when building your website

Consider the following best practices on information security when building an eCommerce website.

Create a page that educates visitors and customers about your website's information security practices and controls. In particular, you should:

- Inform consumers how card account information is protected during transmission, on your server and at your physical location
- Make the page available to all visitors to your website through a link on your home page

Create a "Frequently Asked Questions" (FAQ) page that includes questions and answers on how consumers can protect themselves when shopping online.

If you are using Visa Secure or Mastercard SecureCode, add the logo to your home page, security information page and checkout pages. Also include instructions on how both programs work.

Do not use and advise customers against using emails for transactions. Some customers may wrongly believe that email is a secure way to transmit personal account information. This is actually a non-secure way to do business. In order to protect your customers you should highlight best security practices on your website and in any reply email. In particular, you should inform customers that:

- Email is a non-secure way for transmitting information and should never be used to transmit card account numbers or other sensitive information
- Your website has information encryption capabilities that offer reliable protection from unauthorized access and provide cardholders with the safest way to shop online

Navigating your statement - In one easy guide

1. Header: The header section contains processing month, your unique merchant ID/NBR, DBA name and mailing address.

2. Deposit Summary: It is a line-by-line listing of the daily settlements or batches processed by the merchant for the month. These translate into bank deposits, which include all of the sales for the day's business. The section typically includes the batch date, batch number, batch amount and the amount deposited to the merchant account.

3. Processing Activity Summary: The Processing Activity Summary or General Summary section lists the totals for transactions for each card type being used at the merchant's location. It would list a combination of Visa, MasterCard, Discover and Amex card transactions. There are columns for dollar volume for the month, the number of transactions for the month, credits, net sales, average tickets, qualified rate and total processing fee or discount due.

worldpay
from FIS

xxxxxxxxxxxx

MERCHANT STATEMENT

WORLDPAY INTEGRATED PAYMENTS
150 MERCURY VILLAGE DR.
DURANGO, CO 81301
FOR CUSTOMER SERVICE CALL 1-800-846-4472

PROCESSING MONTH: NOV 2020
MERCHANT NBR: xxxxxxxxxxxx
PAGE 1 of 3

1

DBA NAME: BEST MERCHANT

Attention: JOHN SMITH
SMITH'S
123 SUNNY RD
ROSWELL, GA 12345

2

DEPOSIT SUMMARY

Process Date	Number Sales	Net Sales	Adjustments	Chargebacks	Disc	3rd Party Funded	Net Deposits
03-Nov	0	0.00	0.00	0.00	-27.76	0.00	-27.76
03-Nov	45	564.96	0.00	0.00	0.00	0.00	564.96
03-Nov	55	582.04	0.00	0.00	0.00	0.00	582.04
04-Nov	0	0.00	0.00	0.00	-42.65	0.00	-42.65
04-Nov	143	1,902.36	0.00	0.00	0.00	0.00	1,902.36
06-Nov	0	0.00	0.00	0.00	-57.93	0.00	-57.93
06-Nov	88	1,138.69	0.00	0.00	0.00	0.00	1,138.69
06-Nov	110	1,675.18	0.00	0.00	0.00	0.00	1,675.18
07-Nov	0	0.00	0.00	0.00	-26.63	0.00	-26.63
07-Nov	100	1,180.78	0.00	0.00	0.00	0.00	1,180.78
09-Nov	0	0.00	0.00	0.00	-57.10	0.00	-57.10
09-Nov	98	1,319.35	0.00	0.00	0.00	0.00	1,319.35
09-Nov	108	1,343.91	0.00	0.00	0.00	0.00	1,343.91
Deposits Total	2,131	28,261.18	0.00	0.00	-601.37	0.00	27,659.81

3

PROCESSING ACTIVITY SUMMARY

Card Type	Settled Sales	Amount of Sales	Settled Credits	Amount of Credits	Amount of Net Sales	Average Ticket	Settled Per Item*	Disc Rate	Processing Fees
AMEXOPTBLUE	34	486.64	0	0.00	486.64	14.31	0.0800	0.0800	3.25
DISCOVER	34	487.51	0	0.00	487.51	14.34	0.0000	0.0800	0.56
DISCOVERDEBIT	1	16.61	0	0.00	16.61	16.61	0.0000	0.0800	0.01
MASTERCARD	124	1,850.49	0	0.00	1,850.49	14.92	0.0000	0.0800	2.16
MCDEBIT	515	6,755.36	0	0.00	6,755.36	13.12	0.0000	0.0800	7.38
MCDEBITCAP	238	3,240.01	0	0.00	3,240.01	13.61	0.0000	0.0800	3.59
VISA	252	3,454.68	0	0.00	3,454.68	13.71	0.0000	0.0800	3.89
VISADEBIT	188	2,195.01	0	0.00	2,195.01	11.68	0.0000	0.0800	2.57
VISADEBITCAP	745	9,774.87	0	0.00	9,774.87	13.12	0.0000	0.0800	10.80
Total	2,131	28,261.18	0	0.00	28,261.18	13.26			34.21

* For processor per item fee charged on transaction types other than settled transactions, see Other Fees section below.

Navigating your statement - In one easy guide (continued)

4. Interchange Fees: The non-controllable costs collected on behalf of the card issuer. The card issuer is the issuing bank that provides the consumer with the card being used.

5. Other Fees: Fees assessed on a monthly basis that cover administrative costs of supporting the account. There may also be non-controllable costs from the banks that will be passed thru to the merchant.

MERCHANT NBR: xxxxxxxxxxxx
DBA: SMITH'S

MERCHANT STATEMENT
PAGE 2 of 3
November 30, 2020

4

INTERCHANGE FEES

Description	Number	Amount	Fee Amount
MC CONVENIENCE PURCHASE	25	318.74	6.06
MC DATA RATE I BUSINESS DEBIT	15	226.51	7.07
MC DATA RATE I BUSINESS DEBIT DURBIN FRAUD	13	127.27	2.68
MC DC CPS RESTAURANT-DURBIN FRAUD	66	1,415.88	14.56
MC DC KEY ENTERED-DURBIN FRAUD	9	110.47	1.80
MC DC MERIT III BASE-DURBIN FRAUD	6	263.48	1.44
MC DC SMALL TICKET-DURBIN FRAUD	141	1,293.55	30.68
MC ENHANCED CONVENIENCE PURCHASE	18	262.25	4.52
MC KEY ENTERED - DEBIT	26	300.24	8.27
MC LARGE TICKET LARGE MARKET	2	14.58	0.59
MC MERIT III	1	32.90	0.62
MC MERIT III - DEBIT	10	467.08	5.86
MC MERIT III - PREPAID	1	38.10	0.55
MC RESTAURANT - DEBIT	121	2,576.48	41.81
MC RESTAURANT - PREPAID	10	190.28	3.26
MC SMAL PP DURBIN FRAUD	3	29.36	0.46
MC SMALL TICKET-DEBIT	302	2,715.85	52.31
MC SMALL TICKET-PREPAID	30	240.82	4.94
MC WORLD CONVENIENCE PURCHASE	25	371.15	6.77
MC WORLD ELITE CONVENIENCE PURCHASES	31	498.49	8.89
MC WORLD ELITE KEY-ENTERED	1	29.96	0.85
MC WORLD HIGH VALUE CONV PURCHASES	18	250.29	5.01
MC WORLD KEY-ENTERED	2	27.26	0.76
MC WORLD MERIT III - 1330	1	44.87	0.89
VS BUSINESS CARD CARD PRESENT DURBIN FRAUD	19	252.29	4.40
VS BUSINESS TIER 4 ELECTRONIC	7	173.28	6.54
VS COMMERCIAL CARD RETAIL - PREPAID	1	24.08	0.62
VS CPS RESTAURANT - 1247	10	231.68	4.23
VS CPS RESTAURANT - CK	6	128.04	1.97
VS CPS RESTAURANT - CK-DURBIN	213	4,859.94	47.79
		Total Interchange Fees	531.40

5

OTHER FEES

Number	Amount	Description	Rate	Total
	11,388.29	MASTERCARD ASSESSMENT	0.1300	14.87
	3,343.74	VISACREDIT ASSESSMENT	0.1400	4.66
	11,483.61	VISADEBIT ASSESSMENT	0.1300	14.93
	461.03	DISCOVER ASSESSMENT	0.1300	0.59
	471.41	AMEXNETWORK ASSESSMENT	0.1500	0.71
913		PROCESSOR PER ITEM FEE - AUTHORIZATIONS, MC	0.0800	73.04
1,274		PROCESSOR PER ITEM FEE - AUTHORIZATIONS, VS	0.0800	101.92
37		PROCESSOR PER ITEM FEE - AUTHORIZATIONS, DS	0.0800	2.96
35		PROCESSOR PER ITEM FEE - AUTHORIZATIONS, AX	0.0800	2.80
1		CHARGEBACK SERVICE FEE T1	7.5000	7.50
11		DECLINED AUTHORIZATIONS	0.2000	2.20
37		DISCOVER NETWORK AUTHORIZATION FEE	0.0025	0.09
	29,829.00	EMV NON-ENABLED FEE	0.1500	44.74

Beware of supply scams - Your point of sale staff is your first line of defense

Recently, newly signed merchants received phone calls from businesses representing themselves as the merchant's current credit card processor. The merchants assume that the caller is indeed a representative of their processing bank and consequently do not bother to validate the authenticity of the caller.

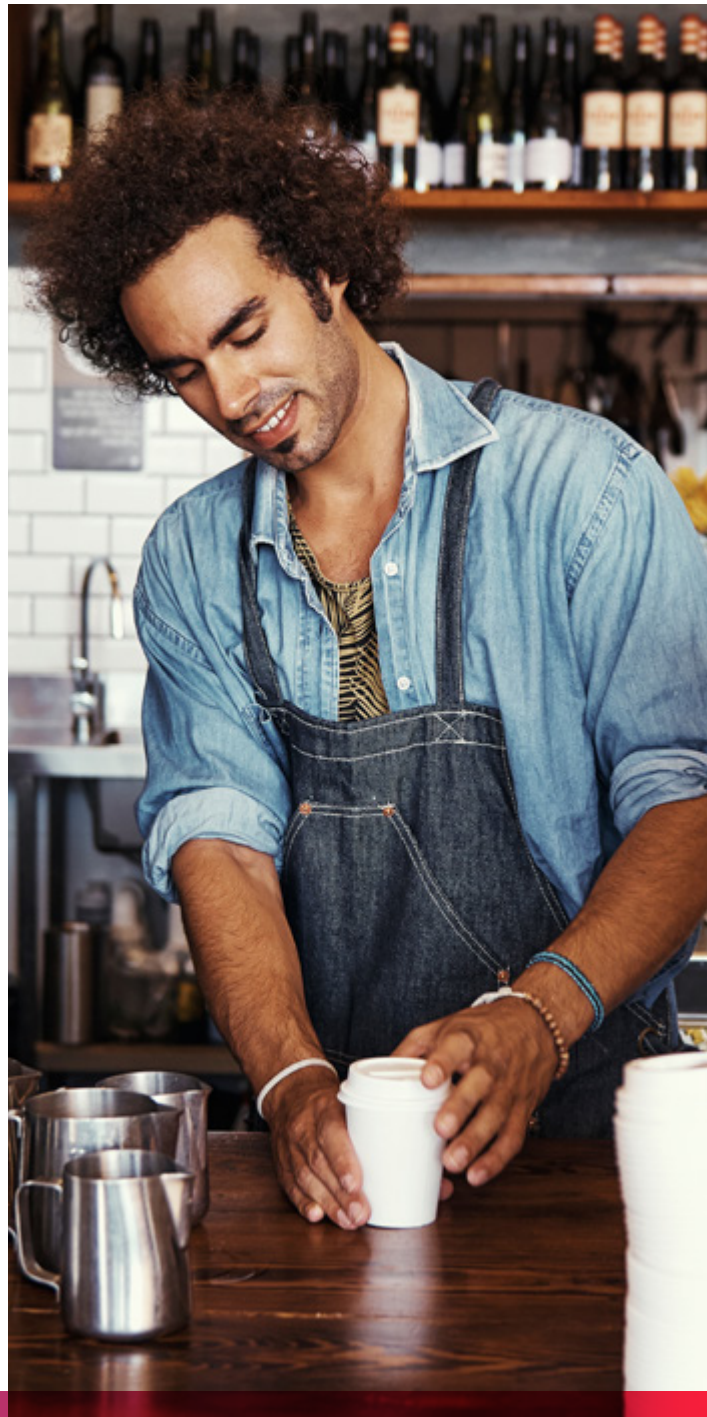
The callers state that they are aware that the merchants have new credit card machines and that they need to perform customer upgrades to their machines. In addition, the callers mention that they have printer ribbons or other supplies they can sell to them at a discounted rate. In most instances, the point of sale staff assumes the callers are legitimate and agrees to the purchase. The merchants then receive the ribbons and are billed exorbitant prices for basic supplies.

This represents one example of many scams regarding supply companies who are charging exorbitant costs for basic supplies. These supply companies are obtaining merchant information illegally and are taking advantage of current and new merchant customers as well. We have taken precautions to ensure that your business information is not compromised.

Steps to take

Don't be taken advantage of this way and remember to take the following steps to ensure that this does not happen to your business.

- Require all callers to clearly identify themselves
- Do not give out credit card numbers over the phone
- Ask if you can phone the caller back if you are suspicious
- Question suspicious behavior such as nervous and shaky voice patterns
- Never allow unauthorized personnel to perform service on your point of sale terminals
- Report suspected fraud to a customer service representative only
- Merchant supplies may be ordered from office supply retailers of your choice



Glossary of terms

Acquirer

An acquirer is an organization licensed as a member of Visa/ Mastercard as an affiliated bank or bank/processor alliance that is in the business of processing credit card transactions for businesses (acceptors) and is always acquiring new merchants.

Address Verification Service (AVS)

The process of validating a cardholder's given address against the issuer's records, to determine accuracy and deter fraud. This service is provided as part of a credit card authorization for mail order/telephone order transactions. A code is returned with the authorization result that indicates the level of accuracy of the address match and helps secure the most favorable interchange rates.

Adjustment

An adjustment is initiated by the acquirer in order to correct a processing error. The error could be a duplication of a transaction or the result of a cardholder dispute. The acquirer debits or credits the merchant DDA account for the dollar amount of the adjustment.

Assessments

Assessments are processing fees merchants pay to the Card Associations to finance their roles in operating the network, setting rules, setting pricing, research and development, and marketing/branding. They are a set percentage of the sale and are generally collected on a daily or monthly basis.

Associations

Any entity formed to administer and promote credit and cards. The best known examples of associations are Mastercard and Visa.

Authorization

The process of verifying the credit card has sufficient funds (credit) available to cover the amount of the transaction. An authorization is obtained for every sale. An approval response in the form of a code sent to a merchant's POS equipment (usually a terminal) from a card issuing financial institution that verifies availability of credit or funds in the cardholder account to make the purchase. Also see point of sale.

Authorization response

An issuing financial institution's electronic message reply to an authorization request, which may include:

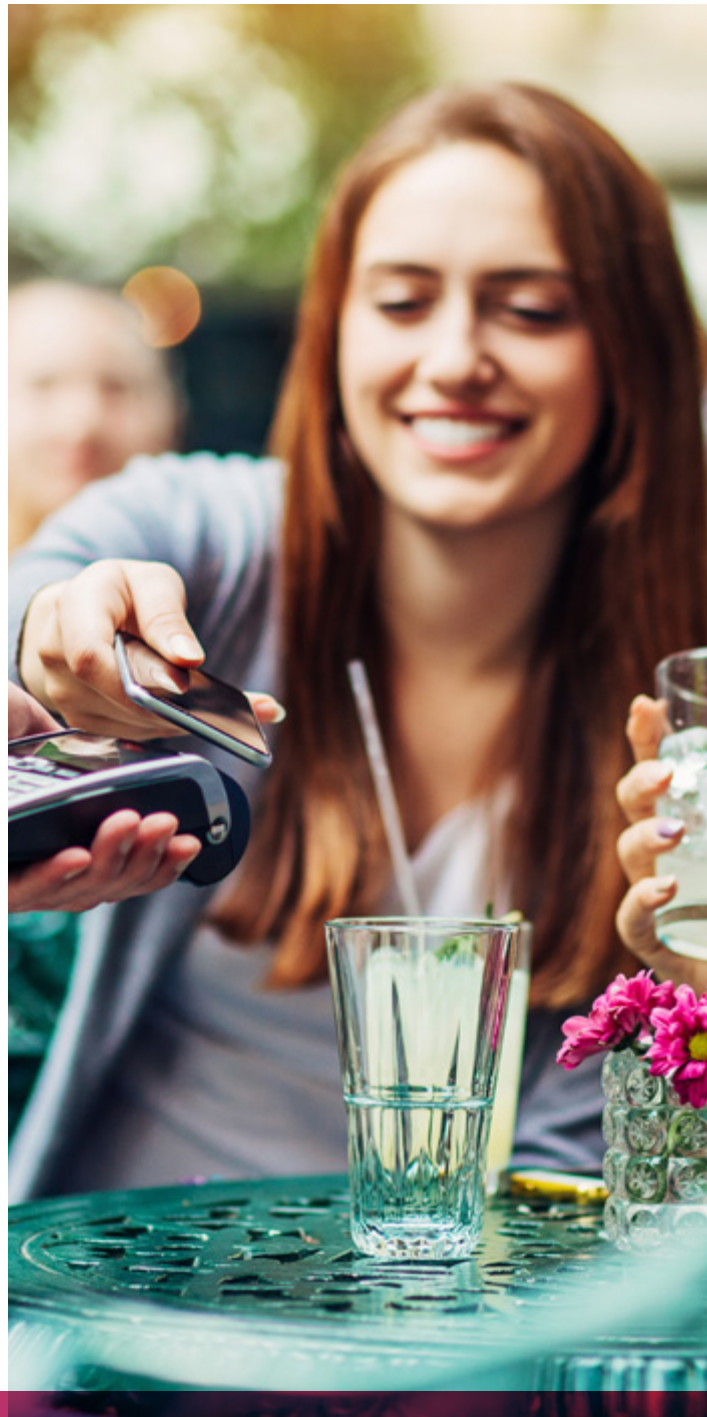
- Approval. Transaction was approved
- Decline. Transaction was not approved
- Call Center. Response pending more information, merchant must call the toll-free authorization phone number.

Automated Clearing House (ACH) file

A file with instructions for the exchange and settlement of electronic payments passed between financial institutions. It represents debits and credits to be deducted from an account automatically as they occur.

Average ticket (average sale)

The average dollar amount of a merchant's typical sale. The average ticket amount is calculated by dividing the total sales volume by the total number of sales for the specified time period.



Glossary of terms

Batch

The accumulation of captured credit card transactions in the merchant's terminal or POS awaiting settlement.

Capture

The submission of an electronic credit card transaction for financial settlement. Authorized credit card sales must be captured and settled in order for a merchant to receive funds for those sales. Also see settlement.

Cardholder data

- Full magnetic stripe or the PAN plus any of the following:
- Cardholder name
- Expiration date
- Service code

Card issuing bank

An EFT Network Member-Bank that runs a credit card or debit card "purchasing service" for their account holders. An example is CitiBank and the CitiBank Visa Card that they issue.

Card not present

A transaction where the card is not present at the time of the transaction (such as mail order or telephone order). Credit card data is manually entered into the terminal, as opposed to swiping a card's magnetic stripe through the terminal.

Card Validation Code 2 (CVC2)

The CVC2 is a three-digit value, which appears at the end of the Mastercard card account number printed in the signature panel that provides a cryptographic check of the card's embossed information.

Card Verification Code 2 (CVV2)

A three-digit value, which appears at the end of the Visa card account number printed in the signature panel that provides a cryptographic check of the card's embossed information.

Chargeback

A credit card transaction that is billed back to the merchant after the sale has been settled. Chargebacks are initiated by the card issuer on behalf of the cardholder. Typical cardholder disputes involve product delivery failure or product/service dissatisfaction. Cardholders are urged to try to obtain satisfaction from the merchant before disputing the bill with the credit card issuer.

Clearing and settlement

The process of exchanging financial transactions details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a customer's settlement position.

Close batch

The process of sending the batch for settlement.

Compromise

Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.

Glossary of terms

Corporate card

Charge card designed for business-related expenses, such as travel and entertainment. Please see commercial card.

Credit (reversal)

Nullification of an authorized transaction (sale) that has not been settled. If supported by the card issuer, a reversal will immediately “undo” an authorization and return it to the open-to-buy balance on a cardholder’s account. Some card issuers do not support reversals.

DDA account

This is the merchants Demand Deposit Account, otherwise known as the merchant’s home town bank account.

Debit card

Payment card whose funds are withdrawn directly from the cardholder’s checking account at the time of sale (online debit on a debit network) or after batch settlement (off-line debit on a credit card network).

Data Encryption Standard (DES)

Block cipher elected as the official Federal Information Processing Standard (FIPS) for the United States in 1976. Successor is the Advanced Encryption Standard (AES).

Deposit account

A deposit relationship between a customer and a financial institution. This includes, but is not limited to, demand deposit (checking), savings, share draft and accounts maintained at the institution.

Discount rate

The percentage of sales amounts that the bankcard acquirer or travel and entertainment (T&E) card issuer charges the merchant for the settlement of the transactions.

Dues and assessments

Dues and Assessments are processing fees merchants pay to the Card Associations to finance their roles in operating the network, setting rules, setting pricing, research/ development, and marketing/branding. They are a set percentage of the sale and are generally collected on a daily or monthly basis.

Electronic Benefits Transfer (EBT)

The distribution of government agency benefits electronically via a plastic Electronic Benefits Transfer (EBT) Card.

Edit rejects

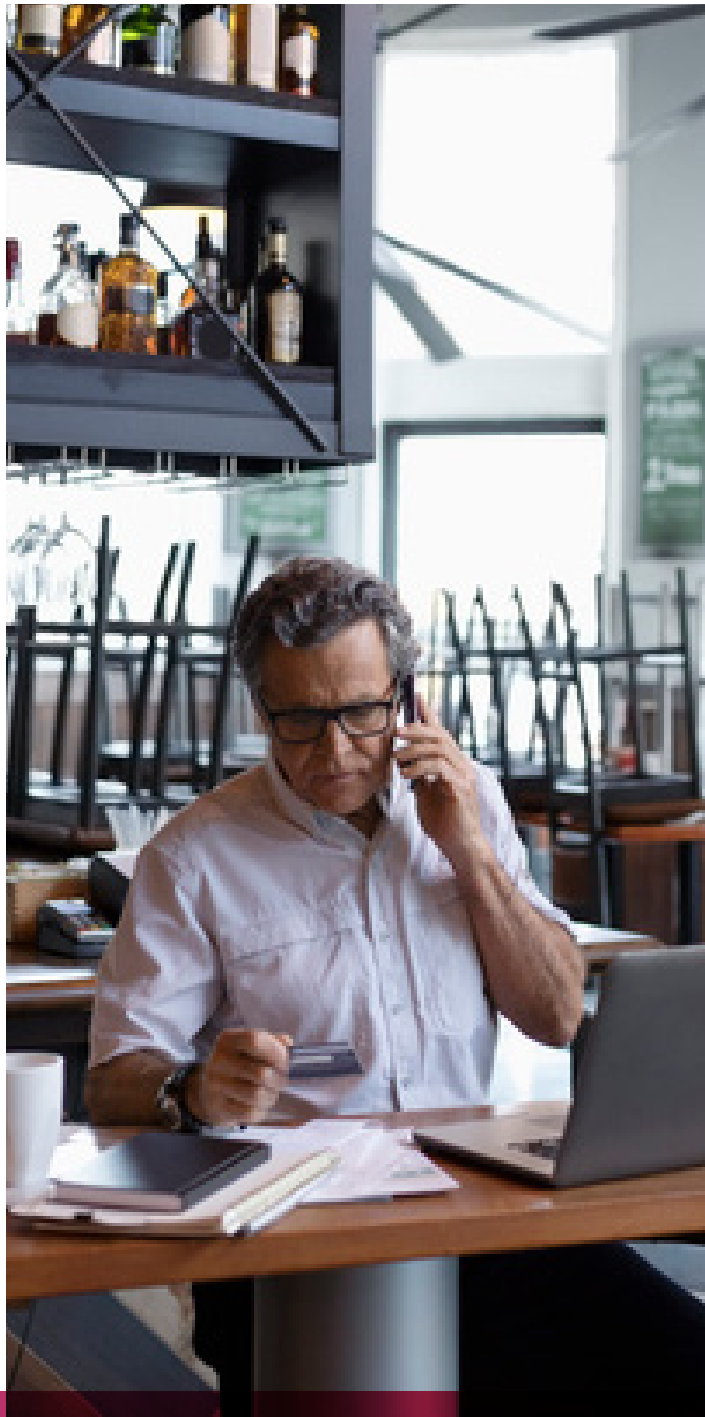
The rejection of a sales draft by Visa or Mastercard before a transaction processes through interchange, but after it has been paid by the acquirer.

Electronic Draft Capture (EDC)

Process of electronically authorizing, capturing and settling a credit card transaction.

Encryption

Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.



Glossary of terms

Exception processing

Any special requirements a merchant has in terms of reporting, accounting, programming or other areas, which necessitate additional work by the processor or acquiring bank.

Expiration date

The date embossed on the card beyond which the card must not be honored.

Fleet cards

Private label credit cards designed for repairs, maintenance and fueling of business vehicles.

Footer

Text printed at the bottom of a sales draft. A merchant can customize the footer (e.g., Have a Nice Day, No Refunds, Thank You for Shopping With Us, etc.).

Host

Offer services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of shopping cart options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server.

Independent Sales Organization (ISO)

An ISO is an Independent Sales Organization that represents a Bank or Bank/Processor alliance. Worldpay is a registered Merchant Services Provider with First National Bank of Omaha.

Interchange fees

The fee that Visa and Mastercard require merchants to pay card-issuing banks for accepting their credit and debit cards.

Issuing financial institution

The bank or other financial institution that extends credit to a cardholder through bankcard accounts. The financial institution issues a credit card and bills the cardholder for purchases against the bankcard account. Also referred to as the cardholder's financial institution. Simply put the issuer is a bank or other institution that issues a credit card or debit card to an individual.

Magnetic stripe

A strip of magnetic tape affixed to the back of credit cards containing identifying data, such as account number and cardholder name.

Mail Order/Telephone Order (MOTO)

Credit card transactions initiated via mail, email or telephone. Also known as card-not-present transactions.

Magnetic stripe data (Track Data)

Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/ Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business.

Glossary of terms

Manual close

A batch close that must be initiated by the merchant on a daily basis, as opposed to an auto close at a pre-set time.

Merchant

A government agency, retailer or any other person, firm or corporation that, pursuant to a merchant agreement agrees to accept credit and/or debit cards when properly presented.

Merchant agreement

A written contract between a merchant and a bank containing their respective rights, duties and warranties, with respect to the acceptance of the bankcard and matters related to the bankcard activity.

Merchant Identification number (MID)

This number is generated by a processor/acquirer and is specific to each individual merchant location. This number is used to identify the merchant during processing of daily transactions, rejects, adjustments, chargebacks, end-of-month processing fees, etc.

Off-line debit (signature debit)

A debit card transaction performed where the purchase is debited from the cardholder's checking account after the clearing and settlement.

On-line debit (PIN debit)

A debit card transaction where a customer uses a Personal Identification Number (PIN) to authenticate the transaction. These transactions are authorized and posted to the cardholder's checking account simultaneously.

Payment Application Data Security Standards (PA-DSS)

The PA- DSS is a security standard created to help software vendors and others develop secure payment applications that do not store prohibited data.

Payment Card Industry Data Security Standards (PCI DSS)

The PCI DSS is a security standard that includes requirements for security management, policies, and procedures.

Payment gateway

A means by which users of one computer service or network can access certain kinds of information in a different service or network.

Point of Sale (POS)

A location where credit card transactions are performed with the cardholder present, such as a retail store. The card is read magnetically, and the cardholder's signature is obtained as insurance against the transaction. This is the most secure form of credit card commerce.

POS terminal

Equipment used to capture, transmit and store credit card transactions at the point of sale. Examples are VeriFone terminals. Examples are Hypercom and VeriFone terminals.

Private label cards

Credit, debit or stored-value cards that can be used only within a specific merchant's store. Private Label cards are also referred to as proprietary cards.

Glossary of terms

Processor

A processor is the company that routes an Authorization Request from a point of sale device to Visa or Mastercard, and then arranges for Fund Settlement to the merchant.

Reference number

The number assigned to each monetary transaction in a cardholder billing system. Each reference number is printed on the monthly statement to help to retrieve the document, should the cardholder question it.

Retrieval request

The request for an original sales slip or legible reproduction of a sales slip as identified in the electronic record.

Sales draft (ticket)

A form showing an obligation on the cardholder's part to pay money (i.e., the sales amount) to the card issuer. This is the piece of paper that is signed when making the purchase. Sales draft data can be captured electronically and sent to be processed over the phone lines. Also see electronic data capture.

Settlement

The process of sending a merchant's batch to the network for processing and payment. For non-bankcards, the issuer pays the merchant directly (less applicable fees) and then bills the cardholder. For bankcards, the acquirer pays the merchant (less applicable fees) with funds from Visa/Mastercard. The bankcard issuer then bills the cardholder for the amount of the sale. Also see capture.

Smart card

A credit-type card that electronically stores the cardholder's account information in the card itself.

Secure Socket Layer (SSL) encryption

Established industry standard that encrypts the channel between a web browser and web server to ensure the privacy and reliability of data transmitted over this channel.

Terminal

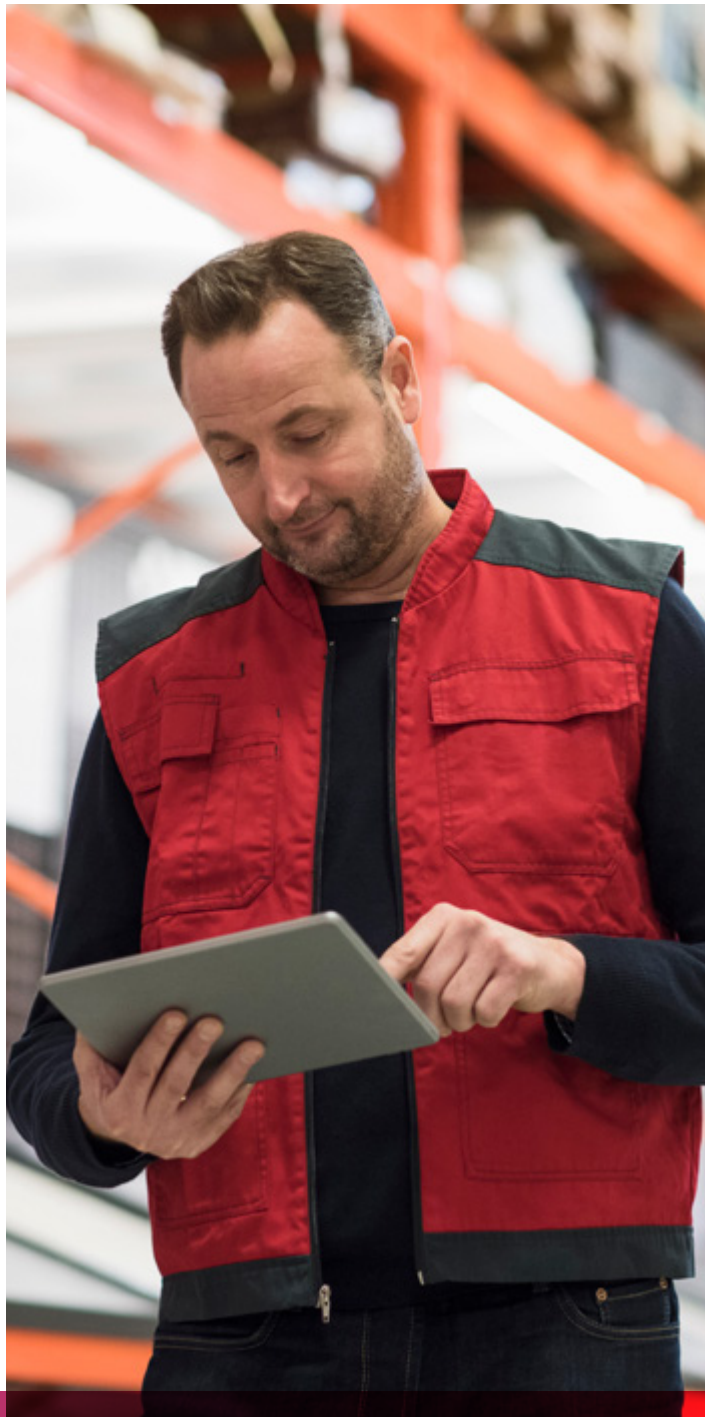
Equipment used to capture, transmit and store credit card transactions.

Travel and Entertainment (T&E) cards

Credit or charge card used by businesses for travel and entertainment expenses. Examples of these cards are American Express, Diners Club, Carte Blanche and JCB.

Zero floor limit

A floor limit that requires all cardholder transactions to be sent to the issuer for authorization.



About Worldpay from FIS

Worldpay from FIS (NYSE:FIS) is a leading payments technology company that powers global commerce for merchants, banks and capital markets. Processing 75 billion transactions topping $9T for 20,000+ clients annually, Worldpay lifts economies and communities by advancing the way the world pays, banks and invests.

We create secure and scalable innovations that connect commerce across all geographies and sales channels. The company's integrated technology platform offers a unified and comprehensive solution set to help clients run, grow, and achieve more for their business.

With a 50+ year history in financial services, we remain ahead of the curve to outpace today's competitive economic landscape. By delivering simple, streamlined, and secure experiences for all of our clients and their customers, we embody commitment to every aspect of the financial services industry.

www.fisglobal.com

twitter.com/fisglobal

getinfo@fisglobal.com

linkedin.com/company/fis

FIS | ADVANCING THE WAY THE WORLD PAYS, BANKS AND INVESTS™