PaymentsFirst
Service • Education • Support

Member Quick Reference
DEBIT AND CREDIT CARD

STANDARD TERMINOLOGY

Access Device: A card, code or other means of account access used by a consumer to initiate electronic funds transfer.
Acquiring Bank: Often called the merchant bank or simply the acquirer. Accepts deposits generated by card transactions for the merchant.
Cardholder: Owner of the card involved in a transaction.
Card Association: A card association is a network of issuing banks and acquiring banks that process payment cards of a specific brand.
Charge Card: No preset spending limit, often do not allow unpaid balances to carry over monthly
Chargeback/Dispute: A forced transaction reversal initiated by the cardholder's bank
Debit Card: A debit card (also known as a bank card, plastic card or check card) may be used when making purchases. Money is immediately transferred directly from the cardholder's bank account when performing any transaction. Minimum charges are not allowed for debit card purchases.
Fallback: Dipping your card, rather than sliding card through card reader. Card Reader is unable to read card when inserted, after second attempt, card falls back to swiped for authorization.
Gateway: A payment gateway is a merchant service provided by an e-commerce application service provider that authorizes credit card or direct payments processing for e-businesses, online retailers, bricks and clicks, or traditional brick and mortar.
Issuing Bank: Financial institution that issues cards, receives payment authorization from card network, approval or declines.
Merchant: Accepts card payments in return for goods and services.
Payment Card Industry Data Security Standard (PCI DSS): Framework developed by PCI Security Standards Council (SSC) for developing robust payment card data security processes.
Payment Processor: Contracts with acquirer to process card transactions.
PIN: Numeric code 4-12 digits used to identify cardholders at activated pin pad.
Secured Card: Initial cash deposit, held by issuer as collateral.
Standard Card: Extended line of credit to cardholders issued by a financial institution which enabling the cardholder to borrow funds. The funds may be used as payment for goods and services. Issuance of credit cards have conditions that the cardholder will pay back the original, borrowed amount plus any additional agreed-upon charges.
Third-Party Service Provider: Used by card-not-present merchants, supplying web hosting, SSL certificates, shopping carts, payment gateway, and more.

RULES AND REGULATIONS

REGULATION E WITH ACCESS DEVICE (DEBIT CARD)

Timing of Consumer Notice to Financial Institutions	Maximum Liability to Consumer
More than 2 business days of learning of loss or theft	Lesser of $50 or total amount of unauthorized transfers
More than 2 business days after learning of loss or theft up to 60 days after transmittal of statement showing first unauthorized transfer made with access device • The day the consumer learns of loss or theft is considered day 0, days 1 & 2 are the following business days	Lesser of $500 or the sum of 1. $50 or the total amount of unauthorized transfers occurring in the first 2 business days, whichever is less, and 2. The amount of unauthorized transfers occurring after the 2 business days and before notice to the financial institution

Event	Timing of Consumer Notice to FI	Maximum Liability to Consumer
Unauthorized transfer(s) not involving the loss or theft of access device (Counterfeit Card)	Within 60 calendar days after transmittal of the periodic statement on which unauthorized transfer first appears	No Liability

Regulation E (Debit Card) Rules established by federal banking regulators and enforced by the CFPB carrying out Electronic Fund Transfer Act, providing consumer rights when cardholder uses financial institution electronic funds transfer system, used by financial institutions to generate debit card transactions. It provides the protections for cardholders using debit cards.

Regulation Z - Truth and Lending Act (Credit Card) Enforced by the CFPB, requires credit card disclosures about its terms and cost. The regulation is designed to protect consumers against misleading lending practices. Under Regulation Z, credit card companies must provide written disclosure of interest rates and finance charges, provide borrowers with explanations of important credit terms, respond to borrowers' complaints about billing, and refrain from engaging in certain unfair lending practices. The error does NOT apply to dispute relating to quality of goods and or services where consumer accepts.

Timing of Provisional Credit *Time Limits Completing Investigations* Financial institution must complete its investigation of an error within 10 business days of receiving a notice of error but may extend 45 calendar days. Investigation must begin promptly, there can be no delays including the receipt of written confirmation. At times, the 10 day period can extend to 20 days and 45 day period can extend to 90 days. A financial institution may require the consumer to give written confirmation of an error within 10 business days of an oral notice. An institution that requires written confirmation shall inform the consumer of the requirement and provide the address where confirmation must be sent when the consumer gives the oral notification. If required written confirmation is not received within the 10 day period, a provisional credit is not due until the consumer comes in and signs the written confirmation.

45 Days After Notice The Issuer provisionally credits the consumers account for the full amount of alleged error plus interest, if any. However, the financial institution may withhold a maximum of $50 of amount credited if financial institution has reasonable basis for believing an unauthorized EFT occurred and complies with liability rules. Informs consumer of amount and date of the provisional credit within 2 days.

EMV - EUROPAY, MASTERCARD VISA

GLOBAL STANDARD FOR CHIP-BASED DEBIT AND CREDIT CARD TRANSACTIONS

EMV POS Counterfeit Fraud Liability		
Chip Capability - Card	Chip Capability - POS	Counterfeit Liability
Magnetic	Terminal Not Contact Chip Enabled	Issuer
Magnetic	Contact Chip Enabled	Issuer
Chip Card	Contact Chip Enabled	Issuer
Countefeit Mag Stripe With Data Copied From Chip Card	Terminal Not Enabled for Contact Chip	Acquiring Bank/Merchant
Counterfeit Mag Stripe With Data Copied From Chip Card	Contact Chip Enabled	Issuer

Lost or Stolen Fraud Present Contact Transactions: Amex, Discover, MC & Pulse		
Chip Capability - Card	Chip Capability - POS	Counterfeit Liability
Magnetic	Any Terminal Type	Issuer
Chip Card, PIN-Preferring CVM (Online or Offline)	Terminal Not Enabled for Contact Chip	Acquiring Bank/Merchant
Chip Card, Signature Preferred	Terminal Not Enabled for Contact	Issuer
Chip Card, Signature Preferred	Contact Chip Enabled Signature No Pin Capability	Issuer
Chip Card, Pin Preferred	Contact Chip Enabled Signature No Pin Capability	Acquiring Bank/Merchant

MASTERCARD DISPUTE

Time Limits: Ensure both the cardholder's and merchants rights are upheld, all groups involved must follow specific time limits, governed by Mastercard and are based on the reason code.

Zero Liability: Applies to purchases made in the store, over the telephone, online, or via a mobile device and ATM transactions. Cardholders are not held responsible for unauthorized transactions if:

- Cardholder used reasonible care in protecting their card from loss or theft; and
- Cardholder promptly reported loss or theft to their financial institution. Zero liability does not apply to Mastercard payment cards: commercial cards, or unregistered prepaid cards, such as gift cards.

VISA CHARGEBACK

Allocation Workflow: Fraud and authorization disputes go through allocation, Visa performs automated checks detecting conditions being met, or dispute process stops. Collaboration Workflow: Assigned for processing error and consumer disputes. Merchants have 30 days to submit a response.

Zero Liability: Requires issuers to replace funds taken from cardholders account as a result of unauthorized credit or debit transaction within 5 days of notification. Cardholders are not held responsible for unauthorized charges made with account or account information. Protections are available for lost, stolen or fraudulent activity when used, online or offline. Does not apply to certain commercial card and anonymous prepaid card transactions or transactions not processed by Visa. Cardholders must use care in protecting their card.

PREPAID CARDS

- Payroll Card Account
- Government Benefits Card Account
- An account marketed or labeled as a prepaid account redeemable for goods or services at unaffiliated merchants or ATM's.
- Reloadable or non-reloadable cards whose primary function is used for similar purposes or to transact Peer-2-Peer transfers.
- Digital Wallets (when wallet itself holds the funds: Venmo, PayPal) Not Apple Pay, Samsung Pay (where credentials are loaded).
- Established disclosure standards are required.
- If account is not registered, financial institutions are not required to resolve errors.
- If account is registered, financial institutions are required to follow Regulation E.

CHARGEBACK PROCESS

Reason Code

Every chargeback must be associated with a reason code that indicates why the original transaction was disputed. Each reason code has its own set of rules for proper/improper use, representment process, filing time limits, and acceptable compelling evidence.

Step 1: Cardholder files a chargeback/dispute with bank issuer asking for refund.

Step 2: Issuer review and assigns a reason code to the dispute case. Each reason code has its own set of rules, filing time limits and necessary documentation.

Step 3: Issuer investigates making sure all regulations are met and it is a valid dispute.

Step 4: Acquirer review the chargeback and takes action.

Step 5: Merchant reviews the chargeback and takes action.

Typical Compliance Violations

- Cardholder stays at lodging merchants location, is later billed as no-show for same location, for same date.
- Merchant adds surcharge as means of payment.
- Merchant bills cardholder for dishonored check.
- Merchant enforces signature of sales draft prior to final dollar amount shown on receipt.
- Cardholder billed advance deposit, amount is not applied to balance of stay.
- Merchant uses another merchants processing terminal, does not have own merchant account.
- Merchant does not capture signature on receipt.
- Cardholder credited more than once for same transaction.

Bank Chargebacks

Cardholder is typically not part of the process on the front end. Bank chargebacks occur when the issuer detects anomaly in the transaction process, triggered by some type of error in the original transaction. There may be a legitimate reason, but the issuer doesn't take the chance and files a chargeback. Examples are

- Declined Authorization
- No Authorization
- Late Presentment
- Lack of required or requested card data
- Incorrect currency or non-matching currency code
- Merchant Fraud
- Non-matching account number

PaymentsFirst Member Support
866-993-3753 info@paymentsfirst.org
678-384-9791 www.paymentsfirst.org

PaymentsFirst
Service · Education · Support