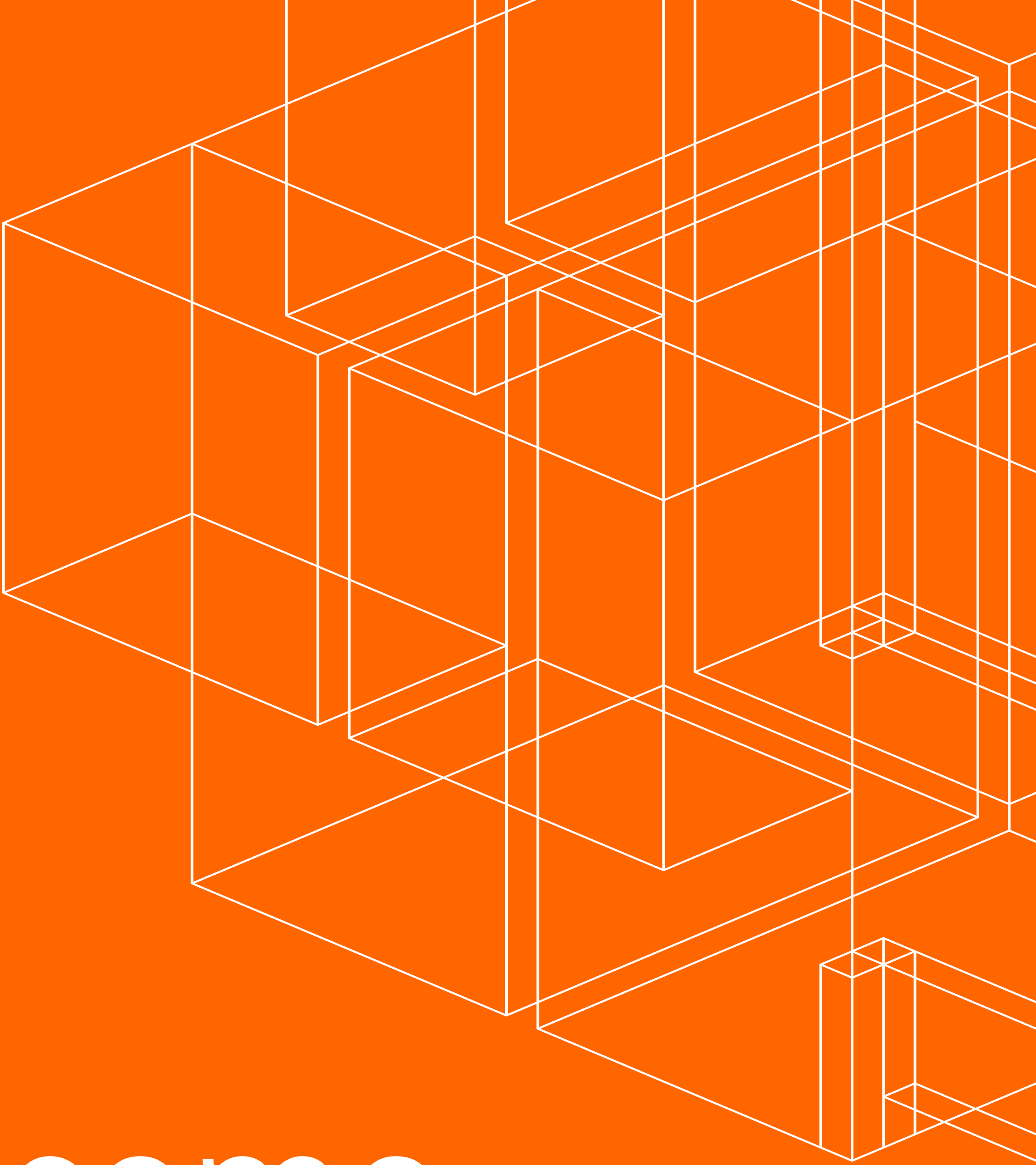


Welcome

IHG Franchisees

IHG® HOTELS & RESORTS

fiserv.

Welcome

Thank you for choosing Fiserv as your IHG NextGen Payments Provider. We look forward to working with you to meet your customers' payment needs. We are committed to providing you with the highest level of service through our strong commitment to quality support and innovative solutions.

We are providing you this Welcome Guide for informational purposes only. The procedures, descriptions, and other content and information contained in this Welcome Guide may change at any time; we have no obligation to notify you of any changes. This Welcome Guide is not a contract or an agreement and does not impact, in any way whatsoever, the terms of our agreement with you. For the avoidance of doubt, all of the terms of our agreement with you, including the terms of the Payments Acceptance Procedures if provided or made available to you, remain in full force and effect as written. If there is any conflict whatsoever between any term or provision of our agreement with you and this Welcome Guide, the terms and provisions of our agreement with you will govern and control (and, in any event, this Welcome Guide is not binding). Any capitalized term used but not defined in this Welcome Guide may be defined in our agreement with you.

If you have any questions regarding your account, please call Customer Service at **866-711-4591**. Again, thank you for choosing Fiserv; we look forward to being part of your continued success.

Contact Information

Customer service

866-711-4591 or franchisepriority@fiserv.com

Please have your merchant ID, phone number and address ready for the account you are calling about.

Merchant activation

For Terminal activation and training

800-558-7101, Option 1

Supply reorder information

Please follow your internal procedures to order supplies. If you are currently required to order supplies from another source, please continue to do so. To reorder supplies, call Customer Service at 866-711-4591, and choose the Customer Service option. Please refer to the Operating Procedures for more information about placing orders for supplies.

Below is a short list of the categories of items we may have available for your processing needs:

- Sales slips
- Credit slips
- Paper rolls
- Ribbons
- Imprinters
- Card Organization decals

Call today for specific product information.

Dispute Resolution

You are required to respond to all chargebacks within the time frames set forth on your notification, regardless of whether you are accepting or refuting liability. To meet dispute requirements, we ask that you use our online tool, Dispute Manager, to receive and respond to dispute notifications online. With Dispute Manager, you receive your dispute information faster and have an archive of dispute documentation, providing easy and secure access to information during the dispute cycle. You may self-enroll in Dispute Manager at the Business Track® portal (businesstack.com), or contact your business consultant or usual customer service area.

Retrieval responses should be faxed to: 402-933-1525

Chargeback responses should be faxed to: 402-933-1840

Equipment Troubleshooting

If you do not purchase hardware from us, then please follow your internal procedures for equipment troubleshooting. If you are currently required to contact another source for equipment troubleshooting, please continue to do so. If you purchase hardware from us, then we hope that you never have any trouble with your processing equipment, but should it malfunction, please check the five troubleshooting points below. If the issue is not resolved, please call the Point-of-Sale (POS) Help Desk at 866-711-4591, and choose the Customer Service option.

To resolve equipment problems, first check to be sure:

- The equipment has not been unplugged
- There is power running to the electrical outlet your equipment is using
- If you process transactions over the internet, check your CAT (Ethernet) cable to ensure it is properly connected to the terminal and your router
- The printer is not out of paper
- The terminal's magnetic card reader is not obstructed or dirty:
  - Check this by folding a clean dollar bill around the Card and sliding it through the reader a few times
- You consult the user manual or quick reference guide (QRG) for equipment troubleshooting information

Please note: If you use a third party for authorization services, you should also contact that provider to ensure there are no issues with their service or equipment. When a technical malfunction prevents electronic completion of a transaction, you must call the Authorization Center at 866-711-4591, and choose the Customer Service option. You may then complete a paper transaction by imprinting the Card and obtaining the Cardholder's signature. Once your equipment is functioning again, you will need to enter this paper transaction into your terminal and settle as usual.

ClientLine® Online Reporting

We encourage our clients to enroll in ClientLine, our feature-rich online reporting tool. You will be able to enjoy the convenience of account information 24/7, along with added enhancements like:

→ Reporting Dashboard – Provides a snapshot of your processing information, transactions, adjustments and bank deposits all on one screen. You can view details by simply selecting a date.

→ Report Scheduler – Delivers reports by email in your preferred file format. Obtain any reports as often as you need them – daily, weekly, monthly, quarterly or annually.

Enrollment is easy – Just follow the steps outlined below:

→ Go to businesstrack.com and click on the "Enroll" button.

→ After you click "Begin Enrollment," you will be prompted to complete a verification process, which, in addition to other basic information, requires your merchant account number (also called your MID, or other number specified by us), business checking account number and taxpayer identification number.

→ If you accept the terms and conditions, then you may select "ClientLine Reporting," as well as the "Dispute Manager EFF." The Dispute Manager EFF allows you to manage your retrievals and chargeback requests online.

→ After a few minutes, you will receive an email with instructions to complete enrollment. Your accounts will be set up and you'll be ready to enter your user ID and temporary password (which you will then be required to change).

→ Once your account is set up, we recommend taking the 20-minute online tutorial by clicking "Tutorial" in the upper-right corner of the reporting tool.

→ If you own multiple locations and your current view within ClientLine does not allow you to see all of your locations together, you can contact us to consolidate. Call our Client Services Support (CSS) at **800-285-3978** and ask the representative to chain your MIDs together.

→ Once your Application is approved, please enroll in the Business Track portal for access to ClientLine and Dispute Manager. Together, these tools provide online access to merchant statements, allow you to manage disputes and respond to Chargebacks, and provide you other functionality and information. Within Business Track, we recommend you enroll to receive three types of email alerts: (1) Daily Account Summary; (2) Dispute Activity; and (3) Monthly Statement Availability. If you do not set up your Business Track account and enroll in Dispute Manager, you will not be able to challenge Chargebacks or address other disputes (other than through mail or fax).

If you have any questions while setting up your account or as you are using ClientLine, call the ClientLine Technical Support Help Desk at **800-285-3978** – available Monday through Friday 8:00 a.m. to 10:00 p.m. ET.

Card Acceptance Information

Please refer to the Operating Procedures or Operating Guide, as applicable (referred to in this document as the "Operating Procedures") for general information about card acceptance (such as (CP) and (CNP) transactions, authorizations and PIN Debit reversals).

Authorization information

All Card transactions require authorization for the full amount of any sale, except in the case of split-tender transactions where a portion of the total transaction amount is submitted for authorization and the remainder is made up with another form of payment. It is up to individual businesses to decide if they will allow split-tender transactions. Authorization indicates that account funds are available and a Card has not been reported as lost or stolen. The authorization process usually takes only a few seconds and allows the Issuer to approve or decline a transaction which helps to protect you from fraud. However, it is not proof that the transaction was made by the true Cardholder or with a valid Card, and so it is not a guarantee against fraud or a future chargeback. The response to your authorization could be any of the following:

Approved: Proceed with the transaction. This is the most common response with most authorization requests being approved by the Card Issuer.

Declined or Card Not Accepted: The transaction cannot be completed with that Card and must not be resubmitted. Request another form of payment and return the Card. The Cardholder will need to call their Card Issuer for more information.

Obtaining Authorization Using the Authorization Center

You should use the Authorization Center if your terminal is inoperable or cannot access the authorization system.

If your POS system supports the functionality, below are the instructions to obtain an authorization from the Authorization Center using a touch-tone phone. Please read through these instructions, so you will know what information to have available before you call 866-711-4591, then follow the prompts for specific needs.

You'll hear	You enter
1. “To obtain a new Authorization, Press 1. For Address Verification, Press 2. For Cardholder bank phone number, Press 3. To go back to the previous menu, Press #.”	Select the appropriate number for your transaction.
2. “Enter the pound sign (#) after each entry.”	
3. “Enter the Credit Card number.”	Customer's Visa®, Mastercard®, Discover® or American Express® number and the pound sign (#).
4. “Enter the four-digit expiration date.”	The expiration month and year on the Card and the pound sign (#). For example, a Card expiring on July 30, 2021 would be entered: 0721.
5. “Enter the amount, dollars and cents.”	The sale amount and the pound sign (#). For example: Amount: Enter: $1.00 1 0 0 (#) $31.00 3 1 0 0 (#) $526.03 5 2 6 0 3 (#)

The dollar amount entered will be repeated. To verify it is correct, Press 1. If incorrect, Press 2 and you will be asked to enter the amount again.

Final steps

6. Enter transaction type:
   (1) Face-to-Face Transaction
   (2) Cash Advance
   (3) Mail or Phone Order

7. Listen for an approval code and then record on sales slip. Follow appropriate action for any other response received. If you hear “hold for operator,” please continue to hold. An operator will assist you in completing the call. If you hang up, the voice system does not recognize that you are no longer on the line and transfers a dead call. This can create delays in the system.

8. Select:
   (1) To Repeat the Authorization
   (2) To Authorize Another Transaction
   (*) To Return to the Previous Menu
   (9) To Return to the Main Menu

Additional Information for PIN Debit Transaction Acceptance

To help you comply with the Card Organization Rules, the following should become a part of your daily business practice for accepting PIN Debit Cards. These procedures also will reduce risk to your business and help increase the profitability associated with accepting Debit Cards for payment. Please refer to the PIN Debit section of the Agreement for further information.

You must allow each Cardholder to enter his or her PIN at or near the POS terminal. The PIN-pad should be placed in a reasonable location, so that Cardholders can enter their PIN without being observed by you or other customers.

Do not require a Cardholder to provide additional identification, information or signature when a Debit Card is properly presented and can be validated by a PIN.

The Cardholder must not tell you his or her PIN verbally or in writing.

→ Participation. You may accept Debit Cards requiring use of a PIN once approved by the applicable Debit Network and in accordance with their Rules.

→ PIN Card acceptance. All PIN-Based Card transactions must be electronically read (swiped). Numbers displayed on the monitor or receipt should be checked against those on the Card being presented for payment. If your terminal does not display the Card number when swiped, please contact our Terminal Support area so that they can update your terminal.

→ IPIN and signature. When there is a technical malfunction that prevents PIN validation, you may at your risk elect to initiate a signature-based (non-PIN) transaction. For these transactions, the Cardholder must provide a signature.

→ Cash back transactions. Any purchase with a cash back transaction must occur in a CP environment and must be verified using the Cardholder's PIN. If you allow Cardholders to initiate cash back transactions through the Debit Network, you must transmit in the Sales Draft the cash amount provided to the Cardholder.

For all PIN-verified purchases with cash back transactions, you should establish a maximum cash back amount. Merchants that offer cash may not set their maximum limit at greater than $200, subject to cash availability, which is in addition to the Cardholder's payment for goods or services.

You must ensure that cash is provided only when combined with a purchase transaction. The purchase, cash back and total transaction components of the purchase with cash back transaction must be in the same currency.

Additional PIN Debit Security Tips

→ Do not log PIN blocks. Although customer-entered PINs are protected in an encrypted form within a transaction message, they must not be retained in transaction journals or logs subsequent to PIN transaction processing. In addition, any temporary logging function for transaction research or troubleshooting must include the active removal of PIN blocks.

→ PIN Entry Devices (PED), have unique keys. By ensuring that these keys are unique to each device, you can make sure your PED are unattractive targets for an attack. PED devices obtained through us and our deployment provider will have unique keys.

→ Educate your employees. Talk to your employees about the potential for PIN compromise if a POS PED is missing or if there are any noticeable signs of device tampering. Inspect the POS PED in service and inventory on a regular basis. You are responsible to secure your terminals and to institute appropriate controls to prevent your employees or anyone else with access to those terminals from processing refunds or voids that do not reflect bona fide returns or reimbursements for prior transactions.

→ Restrict terminal/PED access. Make sure you use only authorized personnel to service deployed terminals and PED. Properly manage PED inventories and physically secure PED at all locations, so they cannot be easily removed, modified or replaced.

→ Use compliant equipment. All PED must be approved under the PCI standards and use the Triple Data Encryption (TDES) algorithm. At no time, may you use PED that has been identified as susceptible to compromise.

Important Information About the Payment Card Industry Data Security Standard (PCI DSS)

Stolen credit and debit Cardholder data due to security breaches at businesses, large and small, has negatively impacted millions of consumers. Your business can be financially responsible if Cardholder data stolen from your business is used fraudulently in any way, including the creation of counterfeit Cards.

Who must comply?

You must comply – all merchants who accept any type of card payment must comply with PCI DSS standards. In addition, you must ensure that any third parties engaged by you ("Merchant Providers") also comply with PCI DSS.

Components of Card Data Security

Implement industry-required data security practices in your business.

→ To help protect payment Card data, the major Card Organizations – including Visa®, Mastercard®, Discover® and American Express® – require all merchants to comply with the security practices found in the Payment Card Industry Data Security Standard (PCI DSS).

→ Complying with the PCI DSS can help merchants prevent data compromises, which may result in Card Organization fines and assessments, plus related fraud losses and other amounts.

→ Applies to all payment Card types, including credit, debit, prepaid and gift cards containing a Card Organization logo. **Use approved payment application software.**

→ The leading cause of Card data compromise incidents for merchants is the use of vulnerable payment applications. Payment applications refer to Card payment processing software installed on a business' computer system, often tied to payroll, inventory and so on.

→ To address this threat, the major Card Organizations require any merchant using payment application software to use versions validated as compliant with the PCI Payment Application Data Security Standard (PA-DSS).

→ Fiserv supports only validated payment applications. For a list of industry-approved applications, please visit: pcisecuritystandards.org/security_standards/vpa.

Use approved terminal devices

→ Increasingly, criminals with sophisticated tools are actively targeting vulnerable merchant POS terminals to steal payment Card data and PINs for counterfeit fraud.

→ If you accept PIN Debit Card transactions, you can help guard against such attacks by ensuring you use only PCI-approved PIN Entry Devices (PEDs).

→ Additionally, all merchants should use POS terminals capable of implementing Card Organization required annual updates, which include fraud prevention enhancements for card present transactions.

Next Steps to Become PCI DSS Compliant[1]

Refer to the table below to determine your PCI level, the required components needed for compliance validation, your validation deadline and the method of contact for your level.

PCI Level	Transaction volume (Visa or Mastercard)	PCI compliance validation documentation	Compliance validation deadline	Method of contact
1	Greater than six million (all channels)	1. Annual on-site audit/Report on Compliance (ROC)[2] 2. Quarterly Network Scan[3] 3. Attestation of Compliance (AOC)	12 months from date of identification and annual revalidation thereafter	Submit compliance validation documentation to assigned GIS analyst or PCI_Compliance@fiserv.com
2	One million to six million (all channels)	1. Annual on-site Self-Assessment Questionnaire or Report on Compliance (ROC)[2] 2. Quarterly Network Scan[2] 3. AOC	12 months from date of identification and annual revalidation thereafter	Submit compliance validation documentation to assigned GIS analyst or PCI_Compliance@fiserv.com
3	Greater than 20,000 eCommerce and less than one million overall Visa and Mastercard transactions	1. Annual Self-Assessment Questionnaire 2. Quarterly Network Scan[3] 3. AOC	12 months from date of identification and annual revalidation thereafter	Submit compliance validation documentation to business consultant if applicable, or email PCI_Compliance@fiserv.com
4	Less than 20,000 in eCommerce only and all other channels up to one million	1. Annual Self-Assessment Questionnaire 2. Quarterly Network Scan[3] 3. AOC	Merchants must maintain PCI compliance at all times including annual revalidation	Maintain PCI compliance at all times. Submit compliance validation documentation annually to your relationship point of contact if applicable, or email PCI_Compliance@fiserv.com Complete your self-assessment through the Trustwave Portal, if you have a Clover Security Plus portal product

[1] This table reflects PCI levels and related information as of the date of the Welcome Guide and may change from time to time.

[2] This must be completed by either a PCI SSC-certified Qualified Security Assessor (QSA) or an Internal Security Advisor (ISA).

[3] Network Scans apply to merchants with external-facing public internet protocols (IP) addresses.

Data compromise procedures

You must immediately notify us of any suspected, alleged or confirmed loss or theft of Cardholder data or transaction information, regardless of the source, including any loss or theft from any Merchant Provider. We and/or the Card Organizations may require you to take additional action. Please contact your Relationship Manager or call Customer Service at **866-711-4591**.

Fiserv is committed to helping our business customers protect themselves from dangerous data compromises that threaten Cardholders' confidential information. We are here to help you navigate the PCI DSS compliance process. The following websites are also very helpful for understanding PCI DSS:

pcisecuritystandard.org

visa.com/cisp

mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html and

discovernetwork.com/merchants/data-security/disc.html

For more information regarding your Data Security requirements and your related responsibilities, please refer to your agreement.

Six Ways to Help Reduce Card Processing Fees

A variety of factors affect the fees associated with Card acceptance. Some factors are beyond your control and ours (for example, if the Card presented has a reward program); others are not. By managing the factors you can control, you can help minimize transactions with higher-than-usual fees, and ultimately reduce your monthly processing expense. The following are tips for reducing your fees:

1. **Settle transactions in a timely manner.**

   If you usually settle transactions more than 24 hours after they are authorized, the interchange and other fees could be higher. Ensure that your terminal is set up to settle Card transactions automatically at the end of your business day. If not, call Customer Service at **866-711-4591** and choose the Customer Service option.

2. **Capture Card numbers by swiping the Card through a card reader or, for chip cards, dipping/tapping the Card.**

   When a customer presents their Card in-person, using a keypad to enter the Card information can lead to higher fees because hand-keyed information is more likely to be entered incorrectly and has a higher potential for fraud.

   What you can do:

   → Obtain a card reader or replace malfunctioning equipment

   → Clean card readers regularly, so they capture all magnetic stripe information. One way to do this is to wrap a dollar bill around a Card and swipe it through the terminal a few times

   → Train personnel to avoid unnecessary key-entered transactions

   → Answer all terminal-prompted questions

3. **Enter the correct ZIP code when a Card number must be hand-keyed.**

   Sometimes, the magnetic stripe on a Card is worn and your card reader is unable to process, and you have to hand-key the transaction. This will result in a higher fee than when a Card is swiped, but you can minimize this fee. When prompted for the ZIP code during a hand-keyed transaction, ask the Cardholder for the ZIP code used for their billing statement. The ZIP code must match the one on record to ensure that you pay the minimum fee for this type of transaction. If this does not match, you may elect to process the Card anyway. There may be a higher risk of fraud, however, and you will pay a higher fee.

4. **Limit CNP transactions.**

   CNP transactions occur when Cardholders provide their Card number and other information over the phone, internet, fax or mail. Since there is no face-to-face interaction or physical signature, these transactions are higher-risk and often result in higher fees.

What you can do:

- → Use the Address Verification Service (AVS) correctly
- → Answer all terminal-prompted questions
  - → You must enter address, ZIP code and an invoice number to receive a more favorable rate
  - → If you do not have an invoice number, we recommend you enter the last-four digits of the card number for reference
- → If you are not prompted to enter address, ZIP code and invoice for a CNP transaction, please call Customer Service at **866-711-4591**, to ensure the AVS and the invoice prompt are activated in your terminal

5 **Limit transaction Authorization and settlement amount mismatches.**

Variation between Authorization and settlement amounts usually triggers additional charges, unless your business is one that commonly processes tips, such as restaurants, taxis or salons. If you are accepting tips at your business, ensure your terminal allows you to add and adjust them. If not, call Customer Service at **866-711-4591**, and choose the Customer Service option. You may not be set up for that type of service.

6 **For our lodging clients: Pass all lodging addenda records including folio information.**

To qualify for CPS Hotel Card Present rates additional data elements must be provided. Folio number, Agreement number and Check-in date must be present. If this data is missing or incorrect Hotel/Lodging transactions will receive a higher interchange level.

We're hopeful that implementing the strategies recommended here will make a noticeable difference in the fees you pay.

Top Nine Card Processing Terms in Plain Language

Total Amount Submitted

The total dollar amount of card transactions submitted and processed during the Statement Period.

Third-Party Transactions

These transactions are passed to a third-party service provider for processing and/or funding.

Adjustments

Amounts credited to or deducted from your account to resolve processing or billing discrepancies.

Interchange Charges

These variable amounts are established by the Card Associations for processing transactions. Factors that influence Interchange Charges include card type, information contained in the transaction, and how/when the transaction was processed.

Service Charges

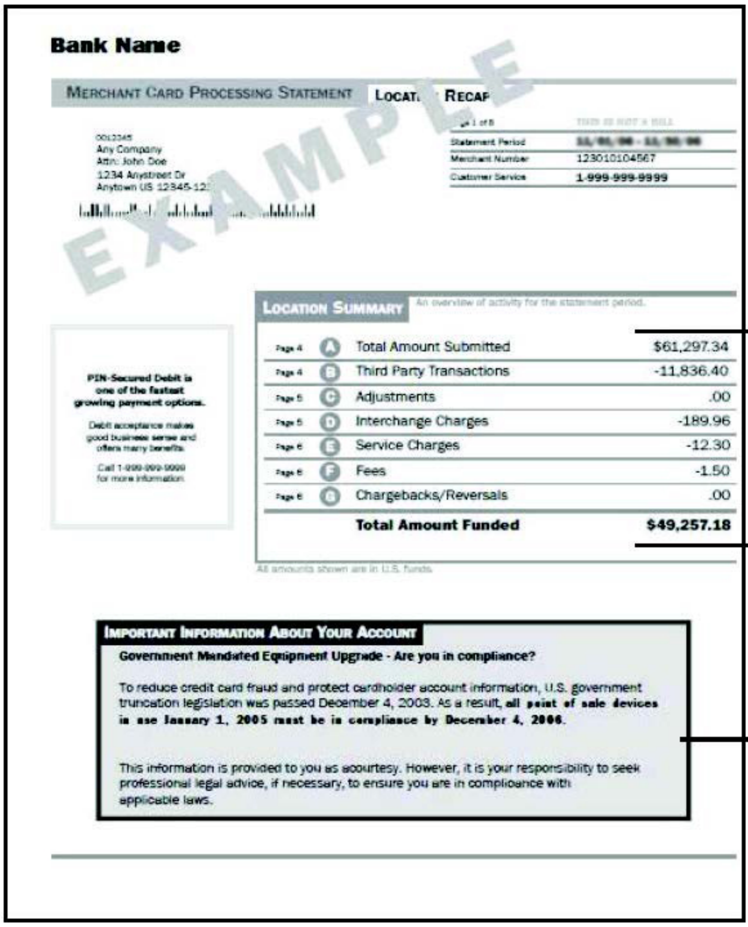
Also known as Discount Rate; amounts charged to authorize, process and settle card transactions.

Fees

A range of transaction – based and/or fixed amounts for specific Card processing services.

Chargebacks/Reversals

Transactions that are challenged or disputed by a cardholder or card-issuing bank. A Chargeback is the amount that is disputed by the cardholder or card-issuing bank. A Reversal is the amount that was previously resolved against the merchant but now is resolved in favor of the merchant.



Bank Name

MERCHANT CARD PROCESSING STATEMENT LOCATI RECAP

EXAMPLE

0012345
Any Company
Attn: John Doe
1234 Anystreet Dr
Anytown US 12345-12

Page 1 of 8	THIS IS NOT A BILL
Statement Period	[illegible]
Merchant Number	123010104567
Customer Service	1-999-999-9999

PIN-Secured Debit is one of the fastest growing payment options.

Debit acceptance makes good business sense and offers many benefits.

Call 1-999-999-9999 for more information.

LOCATION SUMMARY An overview of activity for the statement period.

Page 4	A	Total Amount Submitted	$61,297.34
Page 4	B	Third Party Transactions	-11,836.40
Page 5	C	Adjustments	.00
Page 5	D	Interchange Charges	-189.96
Page 6	E	Service Charges	-12.30
Page 6	F	Fees	-1.50
Page 6	G	Chargebacks/Reversals	.00
		Total Amount Funded	**$49,257.18**

All amounts shown are in U.S. funds.

IMPORTANT INFORMATION ABOUT YOUR ACCOUNT

Government Mandated Equipment Upgrade - Are you in compliance?

To reduce credit card fraud and protect cardholder account information, U.S. government truncation legislation was passed December 4, 2003. As a result, **all point of sale devices in use January 1, 2005 must be in compliance by December 4, 2006.**

This information is provided to you as acourtesy. However, it is your responsibility to seek professional legal advice, if necessary, to ensure you are in compliance with applicable laws.

The **Statement Period** indicates the date range that is included on this statement. Processing that took place within this date range is reported on this statement.

The **Location Summary** summarizes card activity and related charges for the dates specified. Use letters A-G and page numbers to help you quickly find your account details.

When this area appears on your statement, be sure to read it for important information regarding your account.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045
fiserv.com

fiserv.