# Note: The following template can be used to create a UW merchant’s PCI procedures. Please note each merchant is expected to tailor these procedures to fit the specific type of transactions (Card Present, Card-Not-Present, online etc.) and credit card processing equipment and/or POS used by the merchant.

# ACCEPTANCE OF CREDIT CARDS

The University of Wyoming accepts credit cards as payment for goods and services at retail operations around campus and as payment on student accounts for tuition, fees and other University charges. Transactions occur in person, over the telephone and via the internet. The University accepts Visa, MasterCard and Discover at all locations, and American Express at select locations.

**General Operating Guidelines**

The following general guidelines are always applicable to credit card transactions:

1. Do not set restrictions on card transactions: Discover, Visa and MasterCard prohibit setting a minimum or maximum purchase amount. University personnel are also prohibited from adding a surcharge to the transaction amount, but may give a discount from the University’s standard pricing for payment by cash.
2. Protect Cardholder Privacy: The University may only require a Cardholder’s personal information if it is necessary to complete a transaction or if the Voice Authorization Center specifically requests it. University personnel cannot refuse to complete a valid transaction just because the Cardholder refuses to provide additional identification. Any additional information received to complete the transaction should not be written on the purchase receipt.
	1. If University personnel receive a card that has not been signed or says “See ID” in the signature block, the University personnel **must** see additional personal identification to complete the transaction.
3. Keep Cardholder Data Secure: All transaction receipts should be kept in a locked area that is only accessible by select personnel. When receipts are disposed of, be sure that they are disposed of in approved shred bins or with a cross-cut shredder. Receipts should only display the last four digits of a credit card number. Receipts should never contain the customer’s full credit card number
4. Data Compromise: Notify a supervisor and the Associate Vice President Financial Affairs office immediately if University personnel know or suspect that Cardholder information has been accessed or used without authorization, even if this compromise involves a third party vendor.

**General Card Acceptance Procedures**

Card Present Transactions

Although there are different models of credit card acceptance machines around campus, the general steps to accepting a credit card payment are the same depending on the security features of the transaction card being presented. You will be assisting the University in reducing the risk of processing fraudulent credit card transactions by processing Euro MasterCard Visa (EMV) chip enabled or non-EMV (Euro MasterCard Visa) transaction cards properly. Dual interface credit card terminals have been acquired by all campus merchants in order to have the ability to process EMV transactions. Questions on Payment Card Industry (PCI) Compliance, assistance with a transaction card processing terminal or recent transaction batches should be directed through the Associate Vice President Financial Affairs office to the PCI Team at PCI@uwyo.edu or Aaron Courtney at 766-3205.

1. Swipe a non-EMV card, or dip an EMV card into the chip reader to begin the authorization process. If the customer has presented a non-EMV card, hold the card through the entire transaction. Due to the security features of EMV cards, if an EMV card is presented the customer may keep the card in their possession for the transaction. If the EMV reader is not functioning correctly, the terminal will instruct the customer to swipe the transaction card to complete the sale.
	1. Authorization is required for each transaction to determine if the card number is valid, the card has been reported lost or stolen, and that sufficient credit or funds are available to complete the transaction.
	2. One of the following responses will be received back from the authorization process:
		1. Approval code;
		2. declined code (return card to customer and request another form of payment);
		3. declined pick-up (do not return card to customer), or
		4. Referral/Call Auth (call the Voice Authorization Center 1-800-741-5705 for further instructions).
2. While the authorization is processing and if a non EMV transaction card is presented check the card’s features and security elements to detect any irregularities.
	1. VISA cards should have a hologram of a dove on the front or the back of the card. Certain cards may also have a holographic magnetic stripe on the reverse side of the card. The VISA logo should be blue and gold on a white background, located in either the bottom right, top left or top right corner of the card.
	2. MasterCard cards should have a hologram of two globes on the front of the card, above the MasterCard logo. Alternative card designs have the hologram on the back of the card and the MasterCard logo vertical in the upper right corner of the front of the card.
	3. Card number, expiration date and cardholder name should be embossed on the card, with the lettering raised and colored. All digits should be clear, in a straight line, and be the same size/shape. If a card has been re-embossed, the numbers may appear fuzzy.
	4. VISA card numbers should always start with a 4 and MasterCard card numbers should always start with a 5.
	5. The signature panel on the back of the card has a tamper-evident design. If the panel has been erased and resigned, VOID may be displayed in the background of the panel.
	6. On VISA and MasterCard cards, the 3 digit CVV2 code should be printed in a white box just to the right of the signature panel.
	7. Some cards will print the last 4 digits of the card number in the signature panel. Be sure that they match the front and the receipt and that they do not appear to be altered.
3. If an EMV card is presented, after receiving authorization, remind the customer to remove the EMV card from the chip reader.
4. Obtain the cardholder’s signature on the receipt.
5. Compare the name, last 4 digits of the account number and the signature on the card to those on the receipt.
	1. If any of these items do not match, make a Code 10 call as detailed in the Suspicious Activity section below of this policy.
6. Return card and copy of the receipt to the customer.

**NEVER** process an in-person sale without seeing the credit card. If someone wants to recite the credit card number from memory for you to process, stop the transaction and contact a supervisor.

Card Not Present Transactions

Card Not Present Transactions include mail order, telephone order and electronic commerce transactions. These transactions occur when the card is not physically presented to the merchant at the time of sale.

You must request permission to accept Card Not Present transactions. Contact the Associate Vice President for Financial Affairs office/PCI Team to begin the approval process.

Card Not Present transactions pose a higher risk of fraud and chargebacks, so it is important to take precautions when processing these transactions. Obtain the following information to process the payment:

* Purchaser’s name
* Cardholder billing address
* Shipping address, if different from billing address
* Cardholder’s telephone number
* Cardholder’s account number
* Card expiration date
* CVV2/CVC2/CID number (3 digit code next to the signature panel on the back of the card)

After receiving the credit card information, process the transaction following the specific instructions for the Point of Sale system or device that you are using in your area. **Please note** that the cardholder’s account number and CVV2 information can be maintained only to process the initial authorization and should be destroyed after that use. Do not store in hard copy or electronic format. Enter the CVV2 data directly into the terminal and do not write it down.

A receipt for the transaction should be returned to the cardholder. If it is a mail order or telephone order, print the receipt, note the type of transaction on the signature line, and include the copy of the receipt with the invoice upon shipment of the item. For items paid through an e-commerce site, an electronic receipt of the transaction will be sent to the email address that was collected during the transaction.

Never process a card not present transaction using cardholder data received through email or instant messaging. Should a customer email their credit card information:

Reply to the sender, deleting the credit card information from the reply and inform them that “for their protection and that of the University of Wyoming, policies dictate that credit card information shall not be accepted via email. Please use one of our accepted methods of processing your information: (in-person, online, fax, form, etc).”

Be aware of the following possible signs of fraud. Contact a supervisor if you encounter any of these situations:

* Request delivery to a freight forwarder.
* Request to purchase items that the merchant does not sell (the most common items are laptop computer and cellular phones).
* Use of more than one card for a single transaction (also known as Split Ticket).
* Use of cards that have sequential numbers or patterns.
* Utilize a phone relay service where the cardholder does not speak directly to the merchant.
* Place an order and then call back to place subsequent orders using the same or different cards.

**Settling Transactions**

All credit card transactions should be settled daily and deposit information forwarded to the Cashier’s office. Follow the detailed instructions for the Point of Sale system or device that you are using for the settlement process and instructions from the Cashier’s office for deposit information. Credit Card batch deposits to the Cashier’s office should be conducted daily and may be emailed to the Cashier’s Office at Cashiers@uwyo.edu. A receipt for this deposit will be sent to you via campus mail.

**Credit Transactions**

When reversing a credit card transaction or accepting a return or exchange that was originally paid for with a credit card, the University must issue the credit transaction back to the original card used for payment. The customer should be able to provide you with the original receipt and credit card to process the return. Do not refund a card purchase with cash or check. Do not refund cash or check purchases to a card.

**No Signature Required Transactions**

Certain categories of merchants can process transactions that do not require the signature of the cardholder. On the UW campus, this type of transaction is limited to quick service food vendors. You must request permission to process no-signature transactions. Contact the Associate Vice President Financial Affairs office/PCI Team to begin the approval process. Approved vendors can process qualifying transactions with no signature from the customer and do not have to provide the customer a receipt unless they request it. The following criteria must be met:

1. Transaction amount is less than $25.00.
2. The cardholder is present and the transaction occurs in a face-to-face environment.
3. The full and unaltered content of the card’s magnetic stripe is read and transmitted as part of the authorization; card must be swiped through a card reader, manual entry of the card number is not allowed.
4. One authorization is transmitted per clearing transaction.
5. Applies to domestic (U.S.) transactions only.

**Suspicious activity**

In addition to following all of the standard credit card acceptance procedures, University personnel should also be aware of any customer behavior that appears out of the ordinary. The following list, while not all inclusive, represents potential suspicious activity:

* Purchasing large amounts of merchandise with seemingly no concern for size, style, color or price.
* Trying to distract or rush the clerk during a transaction.
* Making purchases either right when the store opens or just before it closes.
* Questions the sales clerk about credit limits or the Authorization process.
* Signs the transaction receipt in a deliberate or unnatural manner.
* Does not have a driver’s license or provides only a temporary license without a photo – applicable only to card transactions that involve a card that says SEE ID on the signature line.
* Ships purchases to an address outside of the U.S.
* Recites the card number from memory rather than presenting the card itself.
* Asks to see the card again before signing the transaction receipt.

**Code 10 Call**

Peculiar behavior should never be automatically assumed to be fraudulent. University personnel will typically know what kind of behavior is normal for the specific place of business. If University personnel do encounter a transaction that is suspicious, the transaction should be reported by making a “Code 10” call. The term “Code 10” is used so the call can be made at any time during a transaction without arousing a customer’s suspicions. To make a Code 10 call, University personnel should:

* Keep the card in his or her possession during the call.
* Call the voice authorization center phone number (1-800-741-5705) and say, “I have a Code 10 authorization request.” The call may be transferred to UW’s acquiring bank and University personnel will need to verify certain transaction details, but will ultimately be transferred to the card issuer and connected to a special operator. They will ask a series of questions that can be answered with a simple yes or no.
* When speaking to the special operator, answer the questions calmly and in a normal tone of voice. The answers will be used to determine if the card is valid.
* Follow all instructions given by the special operator.
* If the special operator tells University personnel to keep the card, do so only if recovery is possible by reasonable and peaceful means.

If University personnel are not comfortable making a Code 10 call during a transaction or becomes suspicious of the transaction after the customer has left the store, the call can still be made. A Code 10 call made after a transaction may help to stop future fraudulent card use at another retail location.

The following are some specific situations where a Code 10 call would be in order:

* Card security features are missing or irregular, or appear to have been tampered with.
* The last 4 digits of the account number on the receipt do not match the numbers embossed on the front of the card.
* University personnel receive a pick-up response when a card has been swiped for electronic authorization.

If University personnel are asked by an operator to recover a suspicious card, remember the following guidelines:

* Recover the card only if it can be done safely. Never take unnecessary risks.
* Tell the cardholder you have been instructed to keep the card and that he or she may call the card issuer for more information.
* Remain calm and courteous. If the cardholder behaves in a threatening manner, return the card immediately.
* If you successfully recover the card, immediately call the Associate Vice President Financial Affairs office and ask for further instructions.
* Cut the card in half lengthwise, being careful not to damage any holograms, the embossed account number, or the magnetic stripe.
* Send the card pieces directly to the Associate Vice President Financial Affairs office, who will return the card to the issuing bank.

**Use of wireless network connections to transmit credit card data**

Due to the inherent vulnerabilities in wireless network connections, credit card data should never be transmitted using one of these connections; this applies to locations on and off campus. The Payment Card Industry Data Security Standards apply to all systems that store, transmit and process credit card data. While the system processing the credit card transaction may be secure, the system transmitting that data must be secure as well. When accessing an online payment site, University personnel should **always** use a wired and trusted connection to maintain the security of the credit card data for the entire transaction. The same guidelines would apply to the transmission of credit card data over a cellular device.

**Debit Card Transactions**

The University accepts debit cards as payment, as long as the card displays the logo of one of the major card brands (e.g. VISA or MasterCard). Process the payment as a credit card payment using the guidelines above. No additional PIN information is necessary to properly complete these transactions.

**Important Phone Numbers**

Voice Authorization Center 1-800-741-5705

Associate Vice President for Financial Affairs-PCI Team 1-307-766-3205

**Key Reminders\***

1. Never store credit card data anywhere (electronically or on paper).

2. Record the serial number of the credit card terminal (if you are using one) that is being used, and verify it daily.

3. Daily verify the UW tamper evident sticker is in place and that it has not been tampered with before you begin use.

\*must be included in merchant procedures