Cash Advance Requirements & Security Best Practices for Financial Institution Partners

General Information

Security Officers and Branch managers are encouraged to **circulate this information regularly** to remind personnel of important requirements and security recommendations related to branch cash advances. Cash advance fraud criminal rings move throughout the U.S. on a regular basis including areas serviced by Wind River Financial.

Special caution must be used as not to sustain fraud related losses. If in doubt as to the identity of an individual attempting to conduct a cash advance, or the validity of a cash advance, we recommend that the transaction not be completed. We recognize that the decision is yours to make based on your individual institution policy.

EMV/Chip Card Note: If your institution has deployed EMV chip card terminals, always attempt to process transactions as chip transactions first. If the chip card will not read via chip and the terminal indicates to swipe the magnetic stripe, it is your option to do so. The card issuer will configure whether to allow magnetic stripe fallback during setup of their EMV program. If the card turns out to be counterfeit, in most cases, the card issuer will hold the counterfeit fraud liability if they allow magnetic stripe fallback. We recommend that your institution create a policy to address this situation.

In addition to the following information, carefully follow and **complete all prompts** on your credit card terminal which will help fulfill identification and transaction requirements.

- **Cards may be embossed or un-embossed:** Card brand operating rules require that entities authorized to make manual cash disbursements honor both embossed cards and cards that do not bear an embossed name (some of these cards are becoming more common).
- Card brand operating rules require that entities authorized to make manual cash disbursements do so for **any cardholder**, even if the cardholder does not have an existing relationship with the financial institution. *Wind River Financial recommends that your financial institution's policies be followed. We also recommend that if an Address Verification Service **(AVS) No Match** is received on a transaction with a non-customer, that the transaction be voided and not continued (related to specific types of cash advance fraud).*
- Per card brand rules, a **surcharge,** or any other fee, must not be added to the transaction amount.
- Card brand rules indicate that you may **establish a maximum** cash disbursement amount of no less than $5000 per day, per cardholder. *Wind River Financial recommends that your financial institution's cash advance policies be followed.*
- **Declined card:** If a decline is received for a known customer, stop the transaction and ask for another card if you wish to make another attempt. Do not attempt to continually get an approval on the same card as this can lead to a loss. *For a non-customer, consult your financial institution policy. We recommend the individual be turned away in the interest of not causing a loss to your financial institution.*

Cardholder Verification (Required Steps)

- **Review government issued identification** (such as unexpired passport or drivers license) to validate the cardholder's identity. Attempt to hold the credentials until the transaction is complete if it can be done without incident.
- **Verify** that the individual presenting the card resembles the photograph on the identification.
- **Record the government identification** number on the terminal if prompted or on the transaction receipt manually.
- Verify that the **signature on the card matches the signature on the transaction receipt** and the identification presented.
- Ask for the **statement/billing address** for the credit card presented. It should match that of the identification presented. Enter the address into the terminal. If a **No Match** response returns for the Address Verification Service (AVS), stop the transaction. Ask the cardholder why it may not match credit card billing records. The Cardholder should know the billing address of the card presented. If new address information is given, and you wish to proceed with another attempt, void the first transaction and initiate a new one with the new address. *Wind River Financial recommends that if an Address Verification Service No Match is received on a transaction with a non-customer that the transaction is voided and not continued.*

Card Verification (Required Steps)

- Check one or more **card security features** before completing the transaction. Visa, MasterCard, and Discover security features can be found at:

  Visa:
  https://usa.visa.com/dam/VCOM/download/merchants/New_VBM_Acq_Merchant_62714_v5.pdf

  MasterCard:
  http://www.mastercard.com/us/merchant/pdf/MST08004_CardFeatures_r4.pdf

  Discover:
  http://www.discovernetwork.com/merchants/fraud-protection/prevention.html

  American Express:
  https://web.aexp-static.com/sg/content/merchant/pdf/working-with-us/avoiding-card-fraud/check-card-faces/Guide_to_checking_Card_Faces.pdf

- Compare the **first four digits** of the embossed Card number to the four digits **printed** below the card number on the front of the card. They should match. Also, once the transaction is processed, verify that the last four digits embossed on the front of the card match the last four digits that are either displayed on the credit card terminal after swiping the card, or as the last four digits are displayed on the printed receipt. If they do not match, it is a counterfeit card and the transaction should be voided.
- **Record the printed four digits** on the front of the transaction receipt or enter into the terminal if prompted.

Uncertain Cardholder or Card Verification

If cardholder identification or a card's validity is uncertain, see the Guarding Against Fraud tips below.

Do Not:

- Call the number on the back of the card. If the card is counterfeit, the telephone number may route to an accomplice's phone which is a common scam. The accomplice will provide a fake verbal authorization number or trick the employee into taking the credit card terminal off line and generating a fake authorization number.
- Call any phone number provided by the Cardholder
- Accept the cardholder's cell phone even if they say they have a credit card company representative on the line
- Press any keys on your terminal at the instruction of the cardholder. A common scam is for the cardholder to trick the employee into taking the terminal off line and generate a fake authorization number. Dispensing funds in this scenario will lead to a loss.

Minimize Chargebacks

- **Always swipe the card or obtain an imprint of the card**. In the event of a chargeback, this provides proof that a card was present at the time of the transaction. If the card will not swipe, follow your financial institution policy. *Wind River Financial recommends that if a card will not swipe with a non-customer that the transaction is voided and not continued. If the card is un-embossed, do not continue with the transaction.*
- Always **compare the cardholder's signature** on the sales draft to the signature panel on the back of the card. Make sure the signature on the sales draft matches the one on the card. If the card is unsigned, have the cardholder sign the back of the card and provide a signed and government issued photo ID. If the cardholder will not do this, do not accept the card.
- **Check the valid dates** on the card to make sure the card is valid and has not yet expired.
- **Obtain an authorization number** for the full amount of the transaction. A credit card authorization code only means that funds are available to cover the amount requested. It does not mean it is a valid transaction.
- If an authorization is **declined,** do not attempt to split the transaction into smaller amounts, make additional attempts to obtain an authorization, or attempt to force it through. Doing so will risk a loss. If you wish to make another attempt, ask the customer for another card.
- If you receive a **No Match on the address verification**, do not proceed with the transaction. (See additional information under Cardholder Verification above).
- **Compare the first four digits** of the Card number to the four digits **printed** below the card number on the face of the card. Assure that the four digits have been recorded on the transaction receipt either manually or via input during terminal prompting.
- **Verify information on the card**: When the receipt prints, verify the printed name on the receipt to the name embossed on the credit card. They should match.

Guarding Against Fraud

How can you tell when a cash advance may be fraudulent? Here are some red flags.

- **Unusual:** If they explain why the cash is needed and it does not make sense. They may seem unusually nervous. Individuals, including the elderly, are sometimes scammed by online fraudsters into doing cash advances and providing the funds in one way or another.
- **Too Busy to Talk:** They remain on a cell phone the entire time in an attempt not to answer security questions.
- **Rushed**: They try to rush the employee through the transaction so that security procedures are not followed.
- **Appearance Out of Character:** Criminal rings often recruit drug addicted or homeless individuals to travel around the country to conduct fraudulent cash advances on counterfeit cards. Appearance can appear a little 'off' such as clothes not fitting properly, empty purses aside from a single wallet, dirty or un kept fingernails, wigs, etc.
- **Asking for Other Locations:** The individual may ask for nearby locations of other branches for your financial institution or those of another institution. They may ask for policies on cash advance limits.
- **Hesitation**: Hesitate or uncertainty when providing personal identification information such as zip code, DOB, or the spelling of a street can be a flag.
- **Multiple Cards**: A request for a cash advance from more than one credit card.
- **Authorizations**: If you receive a "call" response message, call one of the following numbers. Never call the number on the back of the card, a number provided by the cardholder, or accept the cardholder's cell phone if they indicate that a card company representative is on the phone.

.

Visa/MasterCard 800-291-4840

Discover 800-347-6673

American Express 800-528-2121

Cash advance rules must be carefully followed by a financial institution in order to receive protection from chargebacks resulting in losses. If in doubt as to the identity of the individual presenting a card for a cash advance, or the authenticity of the credit card, we recommend that the transaction be voided and the individual be turned away particularly if a non-customer or a brand new customer. Again, we recognize that your financial institution's policy must govern these decisions.