

THE BOARD OF COUNTY COMMISSIONERS
OF SANTA FE COUNTY

Resolution No. 2022-080

A RESOLUTION
ADOPTING THE SANTA FE COUNTY
ACCEPTANCE OF ELECTRONIC PAYMENTS POLICY

WHEREAS, pursuant to Section 6-10-1.2, NMSA 1978, local governing bodies shall adopt procedures, subject to the approval of the New Mexico Department of Finance and Administration (DFA), on the terms and conditions of accepting payments by credit card or electronic transfer.

WHEREAS, pursuant to Section 6-10-1.2, NMSA 1978, DFA, Local Government Division (LGD), Budget and Finance Bureau (BFB), is streamlining the process on how the Local Governing Bodies submit their internal policies and procedures dealing with the acceptance of payments by credit card or electronic transfers at the local level; and

WHEREAS, Santa Fe County does accept electronic payments for various services and needs to adopt a policy to comply with Section 6-10-1.2, NMSA 1978;

NOW, THEREFORE, BE IT RESOLVED, that the Board of County Commissioners of Santa Fe County hereby adopts the Santa Fe County Acceptance of Electronic Payment Policy as attached hereto as Exhibit 1.

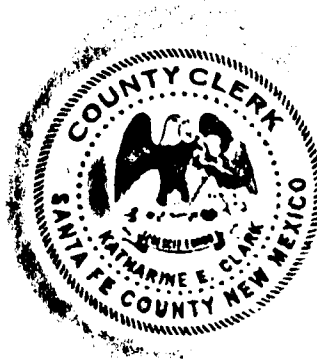
PASSED, APPROVED, AND ADOPTED this 11th day of October, 2022.

BOARD OF COUNTY COMMISSIONERS
OF THE COUNTY OF SANTA FE

By: Anna T. Hamilton
Anna T. Hamilton, Chairperson

ATTEST:
Katharine E. Clark
Katharine E. Clark, County Clerk

APPROVED AS TO FORM:
Jeff Young
Jeff Young, County Attorney



COUNTY OF SANTA FE)
STATE OF NEW MEXICO) ss
I Hereby Certify That This Instrument Was Filed for
Record On The 12TH Day Of October, 2022 at 02:16:31 PM
And Was Duly Recorded as Instrument # 1999331
Of The Records Of Santa Fe County

Deputy Dusty Romero Witness My Hand And Seal Of Office
Katharine E. Clark
County Clerk, Santa Fe, NM



SFC CLERK RECORDED 10/12/2022

Santa Fe County Acceptance of Electronic Payments Policy

Adopted October 11, 2022

I. Introduction

This policy applies to all departments that accept or may accept debit/credit cards or electronic payments for payments of various services provided by Santa Fe County ("County"). The purpose of these procedures is to provide guidance for accepting debit/credit card and electronic transfers for services throughout the County, accounting controls to mitigate risks of credit card fraud, and an understanding of the Payment Card Industry (PCI) regulations.

Section 6-10-1.2, NMSA 1978, provides that a local governing body may accept payment by credit card or electronic means and may charge a uniform convenience fee to cover the approximate costs imposed by a financial institution that are directly related to processing a debit/credit card or electronic transfer transaction.

Debit/credit card customer information is not subject to Public Records Disclosure. Debit/credit card customer information will not be subject to use for commercial purposes.

II. Definitions

1. **Automated Clearing House (ACH)** means an association of depository institutions that process financial transactions electronically through the Federal Reserve Risk.
2. **Convenience Fee** means a fee that is charged to a customer for the convenience of making an electronic payment. A convenience fee charged to a customer typically covers all or a portion of the payment vendor's transaction costs, as well as any other additional fees that are charged by an agency to recover direct costs associated with an electronic payment.
3. **Credit Card** means a card indicating that the holder named on the card has obtained a revolving line of credit from the financial institution issuing the card up to a certain dollar amount valid to a specified date shown on the card. A credit card may be used to pay for goods and services from merchants or organizations participating in the corresponding credit card program.
4. **Debit Card** means a card indicating that the holder named on the card has an open account in a financial institution shown on the card that the holder named on the card is authorized to pay for purchases of goods and services from participating merchants so long as the account is valid and has adequate funds to cover the costs of either goods and services, or both, at the time of the transaction.
5. **Customer** means a person who is purchasing county services with an electronic payment, such as a credit card, debit card or electronic check.
6. **Electronic Check (e-check)** means an ACH debit that is initiated by the customer or agency on the internet against an open account in a financial institution that is authorized for use to pay for purchases of goods and services from participating merchants so long

as the account is valid and has adequate funds to cover the costs of either goods and services, or both, at the time of the transaction. This is also known as an internet check.

7. **Electronic Payments** means any financial transaction by which funds are transferred to the County through any type of electronic payment option or method. The electronic payment options include, but are not limited to; Internet payment processing, point-of-sale payment processing, and interactive voice response (telephone payments). The methods of payment include, but are not limited to; ACH, credit cards, debit cards, ACH debit processing and wire transfers.
8. **Electronic Payment Services** means any service provided by a vendor who acts as an intermediary in processing an electronic payment, including, but not limited to: merchant banking services, credit card payment processing, ACH debit processing, and internet payment gateway services. Depending on how contracts with third party vendors are established, electronic payment services may be coordinated by a single vendor or multiple vendors.
9. **Electronic Payment Processing Protocol** means the standard processes used by the County when accepting electronic payments from customers, including, but not limited to, contracts with financial services providers and business procedures.
10. **Interactive Voice Response System (IVR)** means a system that allows users to pay for services over the telephone or other audio-signal carrier using an electronic form of payment.
11. **Internet Payment Gateway Service** means a service provided by a vendor that directs an internet payment transaction to the appropriate third party payment processor who facilitates the transfer of funds from a specific financial institution.
12. **Merchant Banking Services** refers to the designated bank or banking service that processes an electronic payment.
13. **Payment Vendor** means a service provider who is involved with the electronic payment transaction, including, but not limited to; merchant bank, credit card issuer, credit card association, internet payment gateway, ACH or credit card payment processor.
14. **Payment Card Industry Data Security Standards (PCI DSS)** is the global data security standard adopted by the payment card brands for all entities that process, store, or transmit cardholder data. It consists of common-sense steps that mirror security best practices. Noncompliance to these standards can result in significant fines assessed to the County and may result in loss of the ability to accept credit cards.
15. **Personal Financial Information** means the information provided by the customer in the course of completing a payment transaction with the County through an electronic transfer of funds, including, but not limited to credit card number, debit card number and bank account number.
16. **Point-of-Sale (POS)** is a payment option that performs a real-time payment authorization of a customer's account when the customer presents their credit card (or other payment method) in-person at the time of sale.
17. **Transaction Fee** means the same as "transaction cost" and refers to the cost incurred by a payment vendor for executing an electronic payment. If an agency passes all or a

portion of this transaction cost on to the customer, then the resulting fee to the customer is typically called a convenience fee.

III. Acceptance and Processing

1. Credit card payments shall be used for the sole purpose of processing payment transactions for services provided by the County to the cardholder.
2. New services will be requested through the Finance Division in accordance with these standards. The cost of equipment will be paid from the department's budget, processing fees will be passed on to the card user. Technology implementation must be in accordance with the PCI DSS.
3. Departments must use the credit card payment processor under contract with the County, except for the Utilities Department which is required to use a different credit card payment processor compatible with its billing software. Once the Utilities Department has converted its billing to the County's accounting software, the Utilities Department will be required to use the credit card payment processor under contract.
4. The Finance Division will assist in obtaining new services and equipment working with the contracted credit card payment processor. Departments shall not contact payment processor directly for new equipment or services.

IV. Handling Electronic Payment Information

1. In accordance with PCI DSS, Req. 12.6.1, all employees involved in processing electronic payment transactions and the support of the cardholder data environment (process, review, reconcile, approve, system support, etc.) must be trained upon hire.
2. Protecting cardholder data is essential; thus, every effort shall be made NOT to store cardholder information in any form. Any physical access should be appropriately restricted to data or systems that house, process, or transmit cardholder data to not provide the opportunity for persons to access and/or remove devices, data, systems, or hardcopies.
3. For each Payment Channel, the acceptable PCI DSS compliance method is explained below:
 - a. **Via the phone:** staff is prohibited from taking electronic payments over the phone. The payment service number will be given to the customer, and they will call and make the payment through the secure payment processing center.
 - i. A department/division may ask for an exemption to accept payment information over the phone. Before an exemption will be consider, the Finance Division will discuss with the department/division other available options for processing payments over the phone. If an exemption is approved, the Finance Division will work with the department on establishing procedures to ensure customer information is secure.
 - b. **Via U.S. Mail:** every effort should be made to not accept electronic payment information via U.S. mail. If a payment is received with electronic payment information as form of payment, the staff will reach out to the customer and inform them this payment cannot be processed and give them the phone number to either

SFC CLERK RECORDED 10/12/2022

- pay using the secure phone payment center, and/or the website for online payments to make to secure payment using the secure online payment system.
- c. **In Person:** When processing an electronic payment into the system or POS terminal, it must be processed in full view of the customer. Staff is prohibited from writing or storing card information. Electronic payment information will be processed directly into the system or POS terminal while customer is present at the location. Security controls must be in place when handling in-person transactions. The POS terminal will be turned for accessibility by the card user.
 - d. **Via Fax or Email:** Electronic payment information cannot be accepted via fax or email or any other unsecure communication medium. If a customer does send an email with their card information, the information should be deleted immediately from all email folders. The customer should also be contacted to indicate that the information has been deleted and the transaction has not been processed. The staff member can work with the customer to complete the transaction in an authorized manner.
 - e. **Internet:** Transactions shall be processed through the secure website managed by the IT Division and no information shall be saved/stored.
4. POS terminal equipment shall be stored in a physical secure location when not in use. There shall be a documented and periodic review process in place performed at least quarterly to detect any tampering of equipment (unauthorized payment card skimmers) and a log must be maintained of the periodic review. Upon request by the Finance Division, the Department shall provide the log for review.
 5. In order to ensure compliance with PCI DSS requirement an annual PCI Self-Assessment Questionnaire must be completed and submitted to DFA with the Interim Budget by June 1st of each year.

All standards for the PCI DDS requirements can be found at
<https://www.pcisecuritystandards.org/>

V. Accounting Controls

1. Reporting
 - a. Departments collecting electronic payments will provide reconciled customer payment information to the Finance Division on a weekly basis include payment receipt codes assigned to the appropriate revenue account.
2. Reconciliation
 - a. The Finance Division will reconcile the payment information to the bank activity on a weekly basis.
 - b. The payments will then be receipted in the accounting system and the corresponding batches will be updated to record the activity to the general ledger.
 - c. The electronic payment activity will be included as part of the monthly bank reconciliation.