University Card: Fraud and Disputed Transactions

The following information explains how to identify and report disputed and fraudulent transactions on your University Credit Card.

Deadline for Reporting Transactions

JPMorgan requires all fraudulent transactions to be reported **within 60 days**, with **no exceptions**. Transactions typically appear in Concur within 2–3 business days, and regular monitoring gives ample time to identify duplicate, disputed, or fraudulent transactions and to contact the vendor or JPMorgan as needed.

Disputed Transactions

A *disputed transaction* is one where you, the cardholder, authorized a purchase with a merchant, but the result is incorrect or inconsistent with what was expected.

- Sales tax was erroneously charged, despite providing a tax exemption certificate.
- The amount charged does not match the receipt.
- The items received do not match what was ordered.
- Duplicate transactions where the vendor and amount match exactly, but only one purchase was made.

Fraudulent Transactions

A *fraudulent transaction* is one that you did not authorize, initiate, or permit in any way.

- Your card information was obtained without your consent and used for a charge.
- A thief uses software or algorithms to guess your card credentials.
- Someone other than the named cardholder uses the card. Card sharing is not permitted and should be reported to the Card Administrator.

Tips for Fraud Prevention

- Don’t save your card information in vendor accounts, except were required.
- Avoid using public WiFi for card transactions. Use TCU’s VPN when working remotely.
- Check your Concur profile for transactions at least weekly, and compare them to your receipts obtained at the time of purchase.
- Never share your card information.
- Don’t repeat transactions when your card declines. Call JPMorgan to find out the reason for the decline, and contact the merchant if there are no issues on the bank side.

Questions and Contact Information

- JPMorgan Fraud Contact: 800-895-7074
- Concur Report Help & Card Program Administrator: concur@tcu.edu

Steps for Reporting Fraud

The following sequential process should be followed to report fraudulent transactions found on your card.

1. Confirm the purchase was not an accidental personal charge by checking your personal accounts tied to the vendor.
2. Contact the vendor, if possible, to notify them of the fraudulent charge.
3. Call JPMorgan Fraud at 800-895-7074 and report the transaction. Record the case ID. Provide details of your contact with the vendor, if applicable.
4. Request a replacement card and notify the Card Administrator. This step is intended as a courtesy, and does not exempt you from actioning items in Concur, ordering a replacement card, or reporting the transaction(s).
5. In Concur, code the fraudulent charge using the expense type “Fraud/Disputed Charge” and include the case ID.
6. When the fraud credit appears in Concur, code it using the same expense type and include the case ID. This transaction may go on a separate report if needed.
7. Respond promptly to any follow-up requests from JPMorgan. Failure to respond will result in reversal of the credit, making you/your department responsible for the transaction.

Steps for Reporting Disputed Transactions

Disputes should always begin with the vendor, not JPMorgan. If the vendor does not resolve the issue, you may escalate the case to JPMorgan.

1. For suspected duplicate transactions, confirm the vendor’s name and amount match exactly.
2. Obtain a corrected receipt or request that the vendor adjust the transaction.
3. If you contact the vendor three times without meaningful action, or if they fail to respond to three or more attempts over a period longer than two weeks, report the transaction to JPMorgan.
4. A replacement card is not required for disputed transactions.

Common Kinds of Fraud

The following is a short list of the most common ways fraud transactions occur.

- **Card Not Present Fraud:** A fraudster obtains your card number and uses it for an online purchase.
- **Account Takeover:** A fraudster gains access to your login or card information through stolen credentials, data breaches, or similar methods.
- **Card Skimming:** A device captures your card information from a physical swipe or chip reader.
- **Phishing & Malware:** Fake emails, links, or sites trick you into entering your card or login information.