CREDIT CARD FRAUD CASE ANALYSIS

(simulated portfolio sample)

Role: Fraud Analyst (simulated)

Case Type: Unauthorized Credit Card Transaction

Date: 30 November 2025

This report is a simulated portfolio sample created for training and demonstration purposes only. It is not intended for official or legal use.

1. Case Overview

A customer reported multiple unauthorized credit card transactions made at an online electronics store. The customer confirmed that the card was in their possession, indicating possible card-not-present (CNP) fraud or credential compromise. A fraud investigation was initiated to analyze transaction patterns, verify authentication logs, and determine the method of compromise.

2. Incident Timeline

- **12/09/2025, 10:30 PM:** First unauthorized transaction attempt.
- **12/09/2025, 10:32 PM:** Second transaction — successful.
- **13/09/2025, 08:15 AM:** Customer noticed SMS alerts.
- **13/09/2025, 08:30 AM:** Cardholder contacted customer support.
- **13/09/2025, 08:45 AM:** Card blocked; dispute logged.
- **14/09/2025:** Fraud analyst assigned for investigation.

3. Red Flags Identified

- Transactions originated from a new device not previously associated with the customer.
- IP address traced to another state/country.
- Unusual purchase category: high-value electronics (customer rarely shops online).
- Multiple transactions attempted within minutes.
- No OTP used — possible access to saved card details.
- Delivery address different from customer’s permanent address.

4. Data & Evidence Collected

- Transaction logs and timestamps
- Device ID and IP address details
- Merchant information (payment gateway data)
- Customer's prior transaction history
- Location data from merchant
- OTP logs and authentication history
- Bank card metadata

5. Investigation Approach

1. **Transaction Pattern Analysis-** Compared recent transactions with historical cardholder behavior.
2. **Authentication Check-** Verified OTP
3. **Technical Indicators Review**-Examined device fingerprinting data, IP location, and browser metadata.
4. **Merchant Verification**-Confirmed the legitimacy of merchant and delivery address.
5. **Customer Statement**-Documented customer's dispute and previous card activity.
6. **Fraud Mapping**-Assessed whether the fraud matched known attack patterns (phishing, skimming, data leak).

6. Findings

- Transactions were performed using **card-not-present** method.
- Customer's card credentials were likely compromised through phishing or online data breach.
- Device and IP address used were new and inconsistent with customer's typical usage.
- No OTP was used
- Delivery address belonged to a high-risk zone flagged in previous fraud cases.
- Customer denied all charges and had no history of disputes.

Conclusion: Evidence confirms **unauthorized credit card fraud**.

7. Resolution

- Refund initiated through chargeback process
- Card permanently blocked and reissued.
- Merchant notified to stop delivery of goods.
- Fraud case filed under “CNP Unauthorized Transaction”

8. Recommendations

For bank/customer:

- Enable OTP for all transactions.
- Avoid saving card details on websites.
- Do not click unknown links or share card info.
- Use secure/verified shopping platforms.
- Review statements regularly.

For organization:

- Strengthen fraud detection rules for high-value online transactions.
- Implement AI-based anomaly detection for new devices.
- Monitor transactions from high-risk IP ranges.

Prepared by :

Name & Signature of the officer with date