Jones Automation

a. An automation file is attached.

b.

a. Issues with the UI Mock-Up

1. Security Issues

1. **No HTTPS Indicator**: Users cannot confirm the form is secure.
2. **No CVV Field**: Missing a CVV input makes the form non-compliant with standard credit card security practices.
3. **Unmasked Sensitive Data**: Credit card numbers are not masked during entry.
4. **No CAPTCHA**: The form is vulnerable to bot attacks.
5. **No Encryption Mention**: Users are not informed if their data is encrypted.

2. Usability Issues

1. **No Input Format Guidance**: Users are not told the expected format for fields like credit card numbers or postal codes.
2. **Rigid Formatting Requirements**: Fields don't accept common input styles (e.g., spaces in credit card numbers).
3. **Ambiguity in 'MI' Field**: The "MI" (Middle Initial) field is unnecessary and unclear.
4. **Limited Dropdown Options**: Only supports U.S. regions in the "State or Province" dropdown.
5. **Poor Field Alignment**: Misaligned fields make navigation harder.

3. Accessibility Issues

1. **Lack of Screen Reader Support**: No ARIA labels to help visually impaired users.
2. **Poor Color Contrast**: Light blue background and yellow fields don't meet accessibility standards.
3. **Small Buttons and Dropdowns**: Difficult for users with motor impairments.

4. **Error Handling Issues**
    1. **No Real-Time Validation**: Errors are not flagged as users type.
    2. **Unclear Error Messages**: Messages don’t explain the problem or solution.
    3. **No Formatting Validation**: The form doesn’t reject invalid inputs like incorrect credit card lengths.
    4. **No Fallback Mechanism**: Unexpected inputs, such as special characters, are not handled.
5. **Design Issues**
    1. **Cluttered Layout**: Fields are cramped, making the form look unorganized.
    2. **Not Mobile-Friendly**: The form may not resize properly on mobile devices.
    3. **Unclear Button Hierarchy**: The "Continue" button doesn’t stand out visually.
6. **Performance Issues**
    1. **Dropdowns May Load Slowly**: Particularly on older devices or poor connections.
    2. **No Caching**: Refreshing the page erases previously entered data.
7. **Legal and Compliance Issues**
    1. **No Terms or Privacy Policy**: Missing links to explain data usage or legal terms.
    2. **No Consent Checkbox**: Violates GDPR/CCPA for data collection consent.
    3. **Unclear Charges**: Users don’t know what the $30.00 fee includes.
8. **Localization Issues**
    1. **No International Support**: Doesn’t account for global users (e.g., outside the U.S.).
    2. **Language Limitation**: Only available in English.
    3. **Date Format Ambiguity**: Users may misinterpret expiration date format.

9. **User Feedback Issues**
    1. **No Confirmation Page**: Users can't review their information before submitting.
    2. **No Progress Indicator**: Users don't know how far they are in the payment process.
    3. **No Processing Feedback**: No message reassuring users that their data is being processed.

b. Sample Test Cases

Test Case 1: Validation of Required Fields

- **Objective**: Ensure all mandatory fields display error messages if left blank.
- **Steps**:
    1. Open the form.
    2. Leave all fields empty.
    3. Click "Continue."
- **Expected Result**: Error messages such as "This field is required" appear for all mandatory fields.

Test Case 2: Validation of Credit Card Number

- **Objective**: Verify that invalid credit card numbers are flagged.
- **Steps**:
    1. Enter "1234 5678 9012 345A" in the credit card number field.
    2. Click "Continue."
- **Expected Result**: Error message appears: "Invalid card number. Please enter a valid 16-digit number."

Test Case 3: Validation of Expiration Date

- **Objective**: Ensure that expired credit card dates trigger an error.
- **Steps**:
    1. Select an expiration date in the past (e.g., May 2023).
    2. Click "Continue."
- **Expected Result**: Error message appears: "Card expiration date is invalid."

c. Suggested Product Solution

Most Severe Bug: Lack of Security Features

The absence of HTTPS, CVV fields, and masked inputs puts sensitive user data at risk.

Proposed Solution:

1. **Add a CVV Field**:
    - Make CVV input mandatory.
    - Add a tooltip explaining where to find the CVV on the card.
2. **Implement HTTPS**:
    - Use HTTPS for secure data transmission.
    - Display a padlock icon and “Secure Payment” label.
3. **Mask Sensitive Inputs**:
    - Mask credit card numbers as users type (e.g., **** **** **** 1234).
    - Apply similar masking to the CVV field.
4. **Add Real-Time Validation**:
    - Validate fields (e.g., credit card number, expiration date) as users type.
5. **Tokenization for Credit Card Data**:
    - Replace credit card details with tokens for secure storage and transmission.
6. **Confirmation Page**:
    - Add a summary page for users to review their data before submitting.

By addressing these issues, the form will become secure, user-friendly, and legally compliant.