

SYNTHETIC TEST DOCUMENT — FICTIONAL COMPANY — NO CUSTOMER DATA

Lantern Auto Finance LLC

Identity Theft Prevention / Red Flags Program - DRAFT

Document ID	LAF-ID-004
Version	0.3 (draft)
Drafted	2026-09-12
Owner	Finance and Insurance Manager
Approval status	Not yet approved - no board or senior employee approval recorded
Next scheduled review	Not set in this draft (open item)
Classification	Internal - synthetic test fixture

This document is a synthetic test fixture created for AuditReady page-count, pricing, and pre-scan testing. The company, people, vendors, and events are fictional. It contains no real customer data and no protected health information.

Test intent

A partially written Red Flags program. It names relevant warning signs and responses while explicitly leaving approval, documented risk assessment, service-provider oversight, training evidence, and review timing open. Expanded appendices repeat those open items; they are intentional gaps and are not resolved.

Draft history

Version	Date	Author (role)	Summary of change
0.1	2026-07-02	F&I Manager	Outline of red flags and response steps.
0.2	2026-08-08	F&I Manager	Added detection procedure for application intake.
0.3	2026-09-12	F&I Manager	Added service provider and training notes; approval still pending.

Approval record

Approver	Decision	Date	Evidence reference
Board of directors or appropriate senior employee	Not yet approved	-	None on file

OPEN ITEM (intentional test gap): The Red Flags Rule expects the initial written program to be approved by the board of directors, an appropriate committee of the board, or, if there is no board, an appropriate senior employee. This draft has not been approved by anyone.

Contents

- 1. Business and covered accounts
- 2. Red flags to watch for
- 3. Detection procedure
- 4. Response procedure
- 5. Service providers and training
- 6. Program administration
- 7. Roles (draft)
- 8. Open items register
- 9. Glossary
- Appendix A - Red flag catalog (draft)
- Appendix B - Intake checklist (current version)
- Appendices F onward - Red flag review worksheets and open-item records

1. Business and covered accounts

Lantern is a fictional automobile dealer that offers vehicle financing through retail installment contracts. The company treats consumer financing accounts with multiple payments as covered accounts. The Finance and Insurance Manager is supposed to review new account types each year, but no completed covered-account risk assessment is attached to this draft.

Account type	Covered account?	Basis	Risk assessment on file
Retail installment contract (consumer)	Yes (draft view)	Consumer account with multiple payments	No
Lease referral (consumer)	Undetermined	Not analyzed	No
Business fleet financing	Undetermined	Not analyzed	No
Service department charge account	Undetermined	Not analyzed	No

OPEN ITEM (intentional test gap): No periodic determination of covered accounts is documented. The methods used to open and access accounts, and previous experiences with identity theft, have not been assessed in writing.

2. Red flags to watch for

Employees opening a covered account should look for inconsistent names or addresses, altered identification documents, a credit bureau fraud alert, an address discrepancy, a customer statement that an account is unfamiliar, or a sudden request to redirect account notices. The employee records the flag in the case log without copying a full identity document into the log.

- Alerts, notifications, or warnings from a consumer reporting agency (fraud alert, credit freeze, address discrepancy notice).

- Suspicious documents (identification that appears altered or forged, photo or description inconsistent with the applicant).
- Suspicious personal identifying information (address or phone inconsistent with other sources, SSN not issued or tied to another person).
- Unusual use of, or suspicious activity related to, a covered account (sudden change of address followed by requests for new payment methods).
- Notice from customers, victims of identity theft, law enforcement, or others about possible identity theft.

3. Detection procedure

At application intake, the finance employee compares the applicant's identification and application details and reviews any alert returned by the identity verification service. During account servicing, staff review returned mail and customer complaints. The draft does not specify how to verify a caller asking to change an address, and the current checklist has no field for recording which alert was resolved.

OPEN ITEM (intentional test gap): Caller verification for address change requests is undefined. OPEN ITEM (intentional test gap): The intake checklist lacks an alert-resolution field.

4. Response procedure

When a red flag appears, the employee pauses account opening or the requested change and escalates the case to the Finance and Insurance Manager. The manager may contact the customer through a previously verified channel, request additional evidence, decline the transaction, or contact law enforcement when appropriate. The manager records the decision and reason. The draft contains no deadline for escalation or case closure.

- Monitor the account for evidence of identity theft (draft option).
- Contact the customer through a previously verified channel.
- Change passwords or security codes that permit access to the account (not yet applicable to the dealer portal).
- Decline to open a new account, or close an existing account.
- Notify law enforcement where appropriate (no criteria defined).
- Escalation deadline: not defined (OPEN ITEM (intentional test gap)).

5. Service providers and training

The credit application platform is a service provider involved in covered accounts. The current contract has not been reviewed for red flag detection or reporting duties. New finance staff receive verbal training; there is no training attendance log or refresher schedule.

Service provider (fictional)	Activity	Contract reviewed for Red Flags duties	Evidence
DealDesk Credit Apps	Credit application intake	No	None
VerifyNow ID	Identity verification alerts	No	None
Lienhold Servicing	Payment servicing (proposed)	No	None

OPEN ITEM (intentional test gap): No oversight of service provider arrangements is documented. OPEN ITEM (intentional test gap): Training is verbal only, with no attendance log and no refresher schedule.

6. Program administration

The Finance and Insurance Manager plans to report identity theft trends to senior management annually. The board or an appropriate senior employee has not approved this draft. No annual report, program effectiveness review, or update record exists yet.

7. Roles (draft)

Role	Draft responsibility	Status
Finance and Insurance Manager	Owns the draft; receives escalations; plans annual report	Assigned informally
Finance employees	Check identification and alerts at intake; log red flags	Verbal instruction only
Office staff	Review returned mail and complaints	No written instruction
Board / senior employee	Approve program and oversee administration	Not designated

Role	Draft responsibility	Status
Program administrator	Day-to-day oversight and updates	Not designated

8. Open items register

#	Open item	Owner	Target date
1	Obtain approval of the initial written program	Unassigned	Not set
2	Document covered-account risk assessment	F&I Manager	Not set
3	Define caller verification for address changes	Unassigned	Not set
4	Add alert-resolution field to intake checklist	Unassigned	Not set
5	Set escalation and case-closure deadlines	Unassigned	Not set
6	Review service provider contracts for Red Flags duties	Unassigned	Not set
7	Create training attendance log and refresher schedule	Unassigned	Not set
8	Schedule periodic program update and annual report	F&I Manager	Not set

9. Glossary

Term	Meaning in this draft
Covered account	A consumer account primarily for personal, family, or household purposes that involves multiple payments or transactions.
Red flag	A pattern, practice, or specific activity that indicates the possible existence of identity theft.
Identity theft	Fraud committed or attempted using identifying information of another person without authority.
Service provider	A person that provides a service directly to the company in connection with covered accounts.

Appendix A - Red flag catalog (draft)

Category	Example red flag	Detection point	Written response?
CRA alert	Fraud or active-duty alert on credit report	Application intake	Partial
CRA alert	Notice of address discrepancy	Application intake	Partial
Documents	Identification appears altered or forged	Application intake	Partial
Documents	Photo inconsistent with applicant	Application intake	Partial
Identifying info	SSN matches another applicant	Verification service	No
Identifying info	Phone number is invalid or a pager or answering service	Verification service	No
Account activity	Change of address followed by request for added authorized users	Servicing	No
Account activity	Mail repeatedly returned despite active payments	Servicing	Partial
Notice	Customer reports an unfamiliar account	Complaints	Partial
Notice	Law enforcement inquiry	Management	No

Appendix B - Intake checklist (current version)

- Compare government ID to application name, address, and date of birth.
- Review identity verification service result.
- Note any red flag in the case log (do not copy full identity document).
- Escalate to F&I Manager if a red flag is present.
- Field for which alert was resolved and how: NOT PRESENT (intentional test gap).
- Field for escalation time and closure date: NOT PRESENT (intentional test gap).

Appendix F.001 - Red flag review worksheet: Fraud alert included with a consumer report

Red flag category	CRA alert
Red flag	Fraud alert included with a consumer report
Detection point	Application intake (sales desk)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (sales desk) stage, the finance employee is expected to notice 'fraud alert included with a consumer report' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet.

Program administration status

This worksheet for 'fraud alert included with a consumer report' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (sales desk) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0001. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.002 - Red flag review worksheet: Notice of credit freeze in response to a request for a consumer report

Red flag category	CRA alert
Red flag	Notice of credit freeze in response to a request for a consumer report
Detection point	Account servicing - returned mail
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - returned mail stage, the finance employee is expected to notice 'notice of credit freeze in response to a request for a consumer report' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them.

Program administration status

This worksheet for 'notice of credit freeze in response to a request for a consumer report' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - returned mail stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0002. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.003 - Red flag review worksheet: Notice of address discrepancy from a consumer reporting agency

Red flag category	CRA alert
Red flag	Notice of address discrepancy from a consumer reporting agency
Detection point	Credit application platform alert
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the credit application platform alert stage, the finance employee is expected to notice 'notice of address discrepancy from a consumer reporting agency' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager.

Program administration status

This worksheet for 'notice of address discrepancy from a consumer reporting agency' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the credit application platform alert stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0003. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.004 - Red flag review worksheet: Consumer report shows a pattern of activity inconsistent with the applicant's history

Red flag category	CRA alert
Red flag	Consumer report shows a pattern of activity inconsistent with the applicant's history
Detection point	Application intake (F&I office)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (f&i office) stage, the finance employee is expected to notice 'consumer report shows a pattern of activity inconsistent with the applicant's history' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks.

Program administration status

This worksheet for 'consumer report shows a pattern of activity inconsistent with the applicant's history' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (f&i office) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0004. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.005 - Red flag review worksheet: Identification document appears to have been altered or forged

Red flag category	Suspicious documents
Red flag	Identification document appears to have been altered or forged
Detection point	Account servicing - customer calls
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - customer calls stage, the finance employee is expected to notice 'identification document appears to have been altered or forged' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction.

Program administration status

This worksheet for 'identification document appears to have been altered or forged' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - customer calls stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0005. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.006 - Red flag review worksheet: Photograph or physical description on identification is inconsistent with the applicant

Red flag category	Suspicious documents
Red flag	Photograph or physical description on identification is inconsistent with the applicant
Detection point	Management review
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the management review stage, the finance employee is expected to notice 'photograph or physical description on identification is inconsistent with the applicant' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review.

Program administration status

This worksheet for 'photograph or physical description on identification is inconsistent with the applicant' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the management review stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0006. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.007 - Red flag review worksheet: Other information on identification is inconsistent with the credit application

Red flag category	Suspicious documents
Red flag	Other information on identification is inconsistent with the credit application
Detection point	Identity verification service result
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the identity verification service result stage, the finance employee is expected to notice 'other information on identification is inconsistent with the credit application' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag.

Program administration status

This worksheet for 'other information on identification is inconsistent with the credit application' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the identity verification service result stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0007. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.008 - Red flag review worksheet: Application appears altered, or destroyed and reassembled

Red flag category	Suspicious documents
Red flag	Application appears altered, or destroyed and reassembled
Detection point	Complaint handling
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the complaint handling stage, the finance employee is expected to notice 'application appears altered, or destroyed and reassembled' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence.

Program administration status

This worksheet for 'application appears altered, or destroyed and reassembled' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the complaint handling stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0008. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.009 - Red flag review worksheet: Address does not match information from external sources

Red flag category	Suspicious identifying information
Red flag	Address does not match information from external sources
Detection point	Application intake (sales desk)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (sales desk) stage, the finance employee is expected to notice 'address does not match information from external sources' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down.

Program administration status

This worksheet for 'address does not match information from external sources' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (sales desk) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0009. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.010 - Red flag review worksheet: SSN has not been issued or is listed on a death master file

Red flag category	Suspicious identifying information
Red flag	SSN has not been issued or is listed on a death master file
Detection point	Account servicing - returned mail
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - returned mail stage, the finance employee is expected to notice 'ssn has not been issued or is listed on a death master file' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered.

Program administration status

This worksheet for 'ssn has not been issued or is listed on a death master file' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - returned mail stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0010. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.011 - Red flag review worksheet: Address or phone number is associated with known fraudulent applications

Red flag category	Suspicious identifying information
Red flag	Address or phone number is associated with known fraudulent applications
Detection point	Credit application platform alert
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the credit application platform alert stage, the finance employee is expected to notice 'address or phone number is associated with known fraudulent applications' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern.

Program administration status

This worksheet for 'address or phone number is associated with known fraudulent applications' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the credit application platform alert stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0011. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.012 - Red flag review worksheet: SSN or address is the same as that submitted by other applicants

Red flag category	Suspicious identifying information
Red flag	SSN or address is the same as that submitted by other applicants
Detection point	Application intake (F&I office)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (f&i office) stage, the finance employee is expected to notice 'ssn or address is the same as that submitted by other applicants' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts.

Program administration status

This worksheet for 'ssn or address is the same as that submitted by other applicants' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (f&i office) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0012. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.013 - Red flag review worksheet: Applicant cannot provide authenticating information beyond what is in a wallet

Red flag category	Suspicious identifying information
Red flag	Applicant cannot provide authenticating information beyond what is in a wallet
Detection point	Account servicing - customer calls
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - customer calls stage, the finance employee is expected to notice 'applicant cannot provide authenticating information beyond what is in a wallet' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment.

Program administration status

This worksheet for 'applicant cannot provide authenticating information beyond what is in a wallet' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - customer calls stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0013. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.014 - Red flag review worksheet: Request to redirect account notices shortly after a change of address

Red flag category	Unusual account activity
Red flag	Request to redirect account notices shortly after a change of address
Detection point	Management review
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the management review stage, the finance employee is expected to notice 'request to redirect account notices shortly after a change of address' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs.

Program administration status

This worksheet for 'request to redirect account notices shortly after a change of address' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the management review stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0014. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.015 - Red flag review worksheet: First payment default on a new retail installment contract

Red flag category	Unusual account activity
Red flag	First payment default on a new retail installment contract
Detection point	Identity verification service result
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the identity verification service result stage, the finance employee is expected to notice 'first payment default on a new retail installment contract' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag.

Program administration status

This worksheet for 'first payment default on a new retail installment contract' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the identity verification service result stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0015. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.016 - Red flag review worksheet: Mail sent to the customer is repeatedly returned while payments continue

Red flag category	Unusual account activity
Red flag	Mail sent to the customer is repeatedly returned while payments continue
Detection point	Complaint handling
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the complaint handling stage, the finance employee is expected to notice 'mail sent to the customer is repeatedly returned while payments continue' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag.

Program administration status

This worksheet for 'mail sent to the customer is repeatedly returned while payments continue' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the complaint handling stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0016. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.017 - Red flag review worksheet: Caller requests address change and payoff quote in the same call

Red flag category	Unusual account activity
Red flag	Caller requests address change and payoff quote in the same call
Detection point	Application intake (sales desk)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (sales desk) stage, the finance employee is expected to notice 'caller requests address change and payoff quote in the same call' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed.

Program administration status

This worksheet for 'caller requests address change and payoff quote in the same call' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (sales desk) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0017. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.018 - Red flag review worksheet: Customer reports an unfamiliar account or unexpected statement

Red flag category	Notice from others
Red flag	Customer reports an unfamiliar account or unexpected statement
Detection point	Account servicing - returned mail
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - returned mail stage, the finance employee is expected to notice 'customer reports an unfamiliar account or unexpected statement' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product.

Program administration status

This worksheet for 'customer reports an unfamiliar account or unexpected statement' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - returned mail stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0018. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.019 - Red flag review worksheet: Law enforcement contacts the dealership about a financed vehicle

Red flag category	Notice from others
Red flag	Law enforcement contacts the dealership about a financed vehicle
Detection point	Credit application platform alert
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the credit application platform alert stage, the finance employee is expected to notice 'law enforcement contacts the dealership about a financed vehicle' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists.

Program administration status

This worksheet for 'law enforcement contacts the dealership about a financed vehicle' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the credit application platform alert stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0019. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.020 - Red flag review worksheet: Identity theft victim provides a report concerning an account

Red flag category	Notice from others
Red flag	Identity theft victim provides a report concerning an account
Detection point	Application intake (F&I office)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (f&i office) stage, the finance employee is expected to notice 'identity theft victim provides a report concerning an account' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review.

Program administration status

This worksheet for 'identity theft victim provides a report concerning an account' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (f&i office) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0020. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.021 - Red flag review worksheet: Fraud alert included with a consumer report

Red flag category	CRA alert
Red flag	Fraud alert included with a consumer report
Detection point	Account servicing - customer calls
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - customer calls stage, the finance employee is expected to notice 'fraud alert included with a consumer report' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved.

Program administration status

This worksheet for 'fraud alert included with a consumer report' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - customer calls stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0021. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.022 - Red flag review worksheet: Notice of credit freeze in response to a request for a consumer report

Red flag category	CRA alert
Red flag	Notice of credit freeze in response to a request for a consumer report
Detection point	Management review
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the management review stage, the finance employee is expected to notice 'notice of credit freeze in response to a request for a consumer report' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved.

Program administration status

This worksheet for 'notice of credit freeze in response to a request for a consumer report' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the management review stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0022. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.023 - Red flag review worksheet: Notice of address discrepancy from a consumer reporting agency

Red flag category	CRA alert
Red flag	Notice of address discrepancy from a consumer reporting agency
Detection point	Identity verification service result
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the identity verification service result stage, the finance employee is expected to notice 'notice of address discrepancy from a consumer reporting agency' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet.

Program administration status

This worksheet for 'notice of address discrepancy from a consumer reporting agency' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the identity verification service result stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0023. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.024 - Red flag review worksheet: Consumer report shows a pattern of activity inconsistent with the applicant's history

Red flag category	CRA alert
Red flag	Consumer report shows a pattern of activity inconsistent with the applicant's history
Detection point	Complaint handling
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the complaint handling stage, the finance employee is expected to notice 'consumer report shows a pattern of activity inconsistent with the applicant's history' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them.

Program administration status

This worksheet for 'consumer report shows a pattern of activity inconsistent with the applicant's history' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the complaint handling stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0024. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.025 - Red flag review worksheet: Identification document appears to have been altered or forged

Red flag category	Suspicious documents
Red flag	Identification document appears to have been altered or forged
Detection point	Application intake (sales desk)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (sales desk) stage, the finance employee is expected to notice 'identification document appears to have been altered or forged' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager.

Program administration status

This worksheet for 'identification document appears to have been altered or forged' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (sales desk) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0025. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.026 - Red flag review worksheet: Photograph or physical description on identification is inconsistent with the applicant

Red flag category	Suspicious documents
Red flag	Photograph or physical description on identification is inconsistent with the applicant
Detection point	Account servicing - returned mail
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - returned mail stage, the finance employee is expected to notice 'photograph or physical description on identification is inconsistent with the applicant' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks.

Program administration status

This worksheet for 'photograph or physical description on identification is inconsistent with the applicant' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - returned mail stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0026. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.027 - Red flag review worksheet: Other information on identification is inconsistent with the credit application

Red flag category	Suspicious documents
Red flag	Other information on identification is inconsistent with the credit application
Detection point	Credit application platform alert
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the credit application platform alert stage, the finance employee is expected to notice 'other information on identification is inconsistent with the credit application' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction.

Program administration status

This worksheet for 'other information on identification is inconsistent with the credit application' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the credit application platform alert stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0027. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.028 - Red flag review worksheet: Application appears altered, or destroyed and reassembled

Red flag category	Suspicious documents
Red flag	Application appears altered, or destroyed and reassembled
Detection point	Application intake (F&I office)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (f&i office) stage, the finance employee is expected to notice 'application appears altered, or destroyed and reassembled' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review.

Program administration status

This worksheet for 'application appears altered, or destroyed and reassembled' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (f&i office) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0028. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.029 - Red flag review worksheet: Address does not match information from external sources

Red flag category	Suspicious identifying information
Red flag	Address does not match information from external sources
Detection point	Account servicing - customer calls
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - customer calls stage, the finance employee is expected to notice 'address does not match information from external sources' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag.

Program administration status

This worksheet for 'address does not match information from external sources' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - customer calls stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0029. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.030 - Red flag review worksheet: SSN has not been issued or is listed on a death master file

Red flag category	Suspicious identifying information
Red flag	SSN has not been issued or is listed on a death master file
Detection point	Management review
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the management review stage, the finance employee is expected to notice 'ssn has not been issued or is listed on a death master file' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern.

Program administration status

This worksheet for 'ssn has not been issued or is listed on a death master file' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the management review stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0030. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.031 - Red flag review worksheet: Address or phone number is associated with known fraudulent applications

Red flag category	Suspicious identifying information
Red flag	Address or phone number is associated with known fraudulent applications
Detection point	Identity verification service result
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the identity verification service result stage, the finance employee is expected to notice 'address or phone number is associated with known fraudulent applications' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts.

Program administration status

This worksheet for 'address or phone number is associated with known fraudulent applications' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the identity verification service result stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0031. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.032 - Red flag review worksheet: SSN or address is the same as that submitted by other applicants

Red flag category	Suspicious identifying information
Red flag	SSN or address is the same as that submitted by other applicants
Detection point	Complaint handling
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the complaint handling stage, the finance employee is expected to notice 'ssn or address is the same as that submitted by other applicants' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment.

Program administration status

This worksheet for 'ssn or address is the same as that submitted by other applicants' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the complaint handling stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0032. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.033 - Red flag review worksheet: Applicant cannot provide authenticating information beyond what is in a wallet

Red flag category	Suspicious identifying information
Red flag	Applicant cannot provide authenticating information beyond what is in a wallet
Detection point	Application intake (sales desk)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (sales desk) stage, the finance employee is expected to notice 'applicant cannot provide authenticating information beyond what is in a wallet' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed. The case log records the flag without copying a full identity document, as the draft instructs.

Program administration status

This worksheet for 'applicant cannot provide authenticating information beyond what is in a wallet' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (sales desk) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0033. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.034 - Red flag review worksheet: Request to redirect account notices shortly after a change of address

Red flag category	Unusual account activity
Red flag	Request to redirect account notices shortly after a change of address
Detection point	Account servicing - returned mail
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the account servicing - returned mail stage, the finance employee is expected to notice 'request to redirect account notices shortly after a change of address' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The case log records the flag without copying a full identity document, as the draft instructs. The identity verification service is a service provider, but no one has confirmed whether it reports red flags to Lantern. The worksheet does not state who may approve an exception when a customer cannot provide additional evidence. Staff in the service department may receive address change calls, but they are not covered by any written instruction. The draft does not say how long case log entries are retained or who may access them. No metrics are collected on how often this red flag is detected, escalated, or resolved. The draft has no process to add new red flags when the dealership introduces a new financing product. No refresher training is scheduled for finance employees who handle this red flag.

Program administration status

This worksheet for 'request to redirect account notices shortly after a change of address' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the account servicing - returned mail stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0034. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.035 - Red flag review worksheet: First payment default on a new retail installment contract

Red flag category	Unusual account activity
Red flag	First payment default on a new retail installment contract
Detection point	Credit application platform alert
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the credit application platform alert stage, the finance employee is expected to notice 'first payment default on a new retail installment contract' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

No refresher training is scheduled for finance employees who handle this red flag. Senior management has not received any written report on identity theft trends involving covered accounts. The response to this red flag depends on the manager's judgment because no decision criteria are written down. Returned-mail review happens when staff notice it; no schedule or log exists for this review. The draft does not set a time limit for escalating this red flag to the Finance and Insurance Manager. No field exists on the intake checklist to record which alert was resolved or how it was resolved. Staff have received verbal instruction on this red flag, but no training attendance log exists. The credit application platform contract has not been reviewed for duties to detect or report this red flag.

Program administration status

This worksheet for 'first payment default on a new retail installment contract' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the credit application platform alert stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0035. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.

Appendix F.036 - Red flag review worksheet: Mail sent to the customer is repeatedly returned while payments continue

Red flag category	Unusual account activity
Red flag	Mail sent to the customer is repeatedly returned while payments continue
Detection point	Application intake (F&I office)
Covered account type	Retail installment contract (consumer)
Escalation deadline	Not defined in draft - OPEN ITEM (intentional test gap)
Alert-resolution field on checklist	Not present - OPEN ITEM (intentional test gap)
Training evidence	Verbal only, no attendance log - OPEN ITEM (intentional test gap)
Approval status	Draft - not approved by board or senior employee

Detection steps (as drafted)

At the application intake (f&i office) stage, the finance employee is expected to notice 'mail sent to the customer is repeatedly returned while payments continue' by comparing the applicant's identification and application details with the identity verification result and any consumer reporting agency alert. If the red flag is present, the employee pauses the account opening or requested change and records the flag in the case log without copying a full identity document. The draft does not explain how the employee should verify a caller, what evidence closes the alert, or how long the employee may wait before escalating.

Response options (as drafted)

- Escalate the case to the Finance and Insurance Manager (no deadline set).
- Contact the customer through a previously verified channel.
- Request additional identification or evidence.
- Decline the transaction or the requested account change.
- Contact law enforcement when appropriate (criteria not defined).
- Record the decision and reason in the case log (closure date field missing).

Reviewer notes - open items

The credit application platform contract has not been reviewed for duties to detect or report this red flag. Caller verification for address change requests is not defined, so staff use their own judgment. No covered-account risk assessment supports the decision to treat this account type as covered. The board or an appropriate senior employee has not approved the response options listed for this red flag. There is no scheduled date to update this worksheet to reflect changes in identity theft risks. The Finance and Insurance Manager intends to summarize this red flag in an annual report, but no report exists yet. Case-closure timing is not defined; open cases have no aging review. Program effectiveness for this red flag has not been evaluated, and no incidents of identity theft have been analyzed.

Program administration status

This worksheet for 'mail sent to the customer is repeatedly returned while payments continue' has not been reviewed by the board of directors or an appropriate senior employee. The Finance and Insurance Manager plans to report identity theft trends annually, but no annual report, program effectiveness review, or update record exists yet. The service provider involved at the application intake (f&i office) stage has not been contractually required to detect or report this red flag.

Worksheet ID LAF-RF-0036. Status: draft, unresolved. These gaps are intentional in this synthetic test fixture for a fictional company and should be reported as gaps by any reviewer.