Identity Theft Prevention Program (ITPP)

Last Updated: Jun 22, 2022

1. Program Purpose & Applicability

It is Marchese Ford of Mechanicville's policy to develop, implement and maintain an Identity Theft Prevention Program (ITPP) to detect, prevent, and mitigate identity theft in connection with the opening of, or access to, covered accounts. For the purpose of this ITPP , "identity theft" occurs when a person commits, or attempts to commit, fraud using the identifying information of another person without their authority. All employees who are either directly or indirectly involved in the opening, processing, accessing, or maintaining of a "covered account" must comply with the policies and procedures outlined in this ITPP. This ITPP applies to such employees at the following locations:

- Marchese Ford of Mechanicville, Inc.

This ITPP is intended to comply with the requirements of the various identity theft prevention rules issued by the Federal Trade Commission (FTC), including those of the Red Flags Rule, Address Discrepancy Rule, Fair and Accurate Credit Transaction Act (FACTA), and the Fair Credit Reporting Act (FCRA). No part of this ITPP or its related policies and procedures should be construed as superseding any legal or regulatory requirement. This ITPP and its related policies and procedures reflect Marchese Ford of Mechanicville's good faith efforts to comply with applicable laws and reduce the potential of identity theft from occurring at one of its dealerships or related businesses.

2. Program Administrator(s)

The Program Administrator(s) are designated employees at the senior management level with expertise in the area of identity theft prevention at the dealership who have been designated to supervise the overall management of the ITPP. Program Administrators have the authority and responsibility to:

- Oversee and manage the development, implementation, and administration of the ITPP.
- Assign specific responsibility for the ITPP's implementation, including, but not limited to, appointing, supervising, and managing the activities of employees and others who have specific responsibilities related to the ITPP.
- Review reports prepared by staff regarding compliance by Marchese Ford of Mechanicville with the Red Flags Rule and this ITPP.

- Approve material changes to the ITPP as necessary to address changing identity theft risks.
- Implement and approve new policies and procedures in furtherance of the goals of this ITPP.
- Exercise management control as necessary to ensure that all relevant operations and employees make compliance with this ITPP an integral part of regular operations.

Marchese Ford of Mechanicville has designated the following individual(s) as Program Administrator(s):

- John Byrne / Comtroller / jbyrne@marcheseford.com

3. Risk Assessments

The Red Flags Rule requires that each type of account opened or maintained by the dealership be evaluated to determine if it poses a reasonably foreseeable risk of identity theft. If so, it must be treated as a covered account. The Rule also requires the identification of all relevant red flags. "Red flags" are defined as any pattern, practice, or specific activity that indicates the possible existence of identity theft. When combined, the evaluation of covered accounts and identification of relevant red flags is referred to as the "risk assessment."

In evaluating its accounts, Marchese Ford of Mechanicville assessed the following:

- The types of accounts Marchese Ford of Mechanicville offers, maintains, or accesses.
- The methods Marchese Ford of Mechanicville employs to open its accounts.
- The methods Marchese Ford of Mechanicville employs to access its accounts.
- Marchese Ford of Mechanicville's previous experiences with identity theft.

In identifying the relevant red flags for each covered account offered or maintained by Marchese Ford of Mechanicville, the following categories of red flags were taken into consideration. Where appropriate, red flags from these categories have been included in the ITPP:

- Alerts, notifications, and other warnings received from consumer reporting agencies or service providers, such as fraud detection services offered by credit bureaus or other vendors.
- The presentation of suspicious documents and identifying information.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notices from customers, victims of identity theft, law enforcement, or any other person regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

In determining relevant red flags, Marchese Ford of Mechanicville has also taken the following into consideration:

- Incidents involving identity theft that Marchese Ford of Mechanicville has experienced.
- Changes and trends in the methods of identity theft.

- Guidance and samples provided by the FTC and other regulatory agencies and automobile trade groups.

4. Covered Accounts

The Red Flags Rule requires dealerships to determine whether it offers or maintains "covered accounts" as defined by the Rule. Marchese Ford of Mechanicville has therefore evaluated each type of account that is maintained and determined if it is a covered account. For the purposes of this ITPP and the Red Flags Rule, a covered account is defined as any extension of credit to a customer, whether for personal, family, household, or business purposes to obtain a product or service. Simple purchases, such as a customer purchasing a part with a personal check or credit card, would not be considered a covered account by this ITPP because it lacks a continuing relationship and is not an extension of credit. Pure cash deals would also not be considered covered accounts.

This ITPP will primarily cover the extension of credit to customers for the purpose of leasing and financing vehicles, which is where the greatest risk of identity theft exists. In other words, for the purposes of this ITPP, "covered accounts" means all lease and retail installment sales contracts where financing is obtained by a customer. Other credit accounts, such as wholesale parts accounts and fleet service, may also be designated as covered accounts but will be addressed to a lesser extent in this ITPP because the risk of identity theft is much lower.

Based on the results of most recent risk assessment and review of Marchese Ford of Mechanicville's past identity theft experiences, it has been determined that Marchese Ford of Mechanicville offers or maintains the following types of covered accounts:

- Consumer retail installment sales contract and lease agreements
- Consumer vehicle subscription deliveries
- Commercial trade credit for wholesale parts
- Consumer credit accounts for service and parts
- Consumer credit card accounts
- Commercial retail installment sales contract and lease agreements
- Commercial trade credit for fleet services
- Consumer credit accounts for rental cars

5. Red Flag Identification, Detection & Response

This section includes each of the relevant Red Flags identified as part of the most recent risk assessment.

For each relevant red flag identified by Marchese Ford of Mechanicville, there are documented detection methods and response procedures. Employees are responsible for following these de-

tection methods and response procedures and will not be authorized to open an account until all red flags have been detected and properly mitigated by the appropriate means.

The detection and response procedures included in this ITPP are updated regularly to ensure they reflect (1) the current trends in identity theft, (2) the current systems and applications used by Marchese Ford of Mechanicville to detect fraud and identity theft, (3) Marchese Ford of Mechanicville's most recent experiences with identity theft, and (4) newly identified risks or covered accounts.

Red Flag #1
A fraud or active duty alert is included with a consumer credit report or red flag summary.
Detection Methods
Check for a fraud or active duty alert on every consumer credit report, even if the alert is not included in the bureau's red flag summary
Response Procedures
1. Ask the customer if they have ever placed a fraud alert on their credit report. 2. Check to see if the telephone number or email stated in the alert matches the contact information provided by the customer on the credit application. 3. Contact the customer using the telephone number or email stated in the alert, if any. 4. Verify the customer's identity and obtain authorization from the customer to proceed with opening the account. 5. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 6. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #2
The credit report or red flag summary provides a notice of credit freeze in response to a request for a consumer report.
Detection Methods
Be alert for a credit freeze notice when obtaining a consumer credit report.
Response Procedures
1. Ask the customer if they have ever had their credit report blocked or frozen. 2. Check to see if the telephone number or email stated in the notice of credit freeze matches the contact information provided by the customer on the credit application.

3. Contact the customer using the telephone number or email stated in the alert.
4. Do not proceed with the transaction unless the customer "thaws" or removes the credit freeze. In most cases, the customer can do this by either providing the dealer with a special PIN number or by visiting the website of the applicable credit bureau and filling out a request to either permanently or temporarily remove the credit freeze. You can normally verify the "thaw" by running a fresh pull on the credit report.
5. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.
6. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #3
The credit report or red flag summary provides a notice of address discrepancy.
Detection Methods
Be alert for an address discrepancy notice when obtaining a consumer credit report. An address discrepancy occurs when the address reported by the customer does not match the current address that the credit bureau has on file. There are many different notices that describe an address discrepancy. The following are some common examples: • No match to name—residential address • Address unverifiable—not in database • Current address—no match
Response Procedures
1. Compare the address used by the customer, as well as previous addresses listed in the consumer credit report, with (1) other documents provided by the customer, such as driver license, vehicle title, personal check, etc., and (2) previous customer account records, if any. 2. Ask the customer for any previous addresses they lived at and compare their answer with what is listed on the consumer credit report. 3. If necessary, request proof of residence from the customer (either utility bill, mortgage statement, or property tax bill). 4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #4

A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as (1) a recent and significant increase in the volume of inquiries, (2) an unusual number of recently established credit relationships, (3) a material change in the use of credit, especially with respect to recently established credit relationship, or (4) an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Detection Methods

Review each consumer credit report for any of the suspicious activity stated above. A significant increase in the volume of credit inquiries is sometimes indicative of identity theft because the thief will often use a "shotgun" approach to obtain as much credit as possible within a short time period.

Response Procedures

1. Request documentation that verifies the information provided by the customer on the credit application (e.g., second form of identification, proof of residence, copy of SSN card, employment information, etc.)
2. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.
3. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #5

Customer's credit report shows "no record found" or similar designation, or out-of-wallet questions are unavailable.

Detection Methods

Be alert for a message of "no record found," "no credit file," or similar alert when obtaining a consumer report. Out-of-wallet questions may also be unavailable.
This may occur for many reasons, including the following:

- The individual is of a young age and has not yet established any credit history. If this is the case, the response procedures listed below may not be necessary.
- The individual has purposely provided false information because he/she has a criminal record or does not want you to view his/her credit report for some other reason.
- The individual is attempting to commit identity theft but provided inconsistent information, resulting in a "no record found" message or similar alert.
- The customer's SSN, date of birth, address, or name was entered incorrectly.
- Customer is a new arrival to the country and has not yet established any credit history or has not established.

Response Procedures
1. Request documentation that verifies the information provided by the customer on the credit application (e.g., second form of identification, proof of residence, copy of SSN card, employment information, etc.) 2. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 3. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #6
Documents provided for identification appear to have been altered or forged.
Detection Methods
Before proceeding with the transaction, obtain and inspect the customer's current driver license or other government-issued photo identification. If involving a legal entity, require documents demonstrating the existence of the entity such as articles of incorporation, government-issued business license, etc. Review the identification documents for signs of alteration or forgery, using available tools, if any, such an ID scanning software or guidebook of sample IDs and verification methods.
Response Procedures
1. Obtain a reasonable and verifiable explanation that explains the appearance of alteration or forgery. 2. Require at least one additional form of government-issued photo identification and one other form of identification. 3. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system. 4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #7
The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

Detection Methods
Before proceeding with the transaction, obtain and inspect the customer's current driver license or other government-issued photo identification. If involving a legal entity, require documents demonstrating the existence of the entity such as articles of incorporation, government-issued business license, etc. Review the identification documents for signs of alteration or forgery, using available tools, if any, such an ID scanning software or guidebook of sample IDs and verification methods.
Response Procedures
1. Obtain a reasonable and verifiable explanation that explains the discrepancy. 2. Require at least one additional form of government-issued photo identification and one other form of identification. 3. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system. 4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #8
Information on the customer's government-issued identification is not consistent with other identifying documents, such as the credit application, proof of income, proof of residence, or other identifying documents.
Detection Methods
Before proceeding with the transaction, obtain and inspect the customer's current driver license or other government-issued photo identification. If involving a legal entity, require documents demonstrating the existence of the entity such as articles of incorporation, government-issued business license, etc. Compare the address, date of birth, full name, and other information of the identification with information provided by the customer in the credit application or other identifying documents.
Response Procedures
1. Obtain a reasonable and verifiable explanation that explains the discrepancy. 2. Request documentation that verifies the information provided by the customer on the credit application (e.g., second form of identification, proof of residence, copy of SSN card, employment information, etc.) 3. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.

4. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #9
Customer's down payment check looks altered, forged, or is written on someone else's account.
Detection Methods
Identity thieves often print fraudulent checks that reflect the checking account and routing number belonging to someone else. The following detection procedures may help identify a fraudulent check: • Compare the first and last name of the customer with the name displayed on the customer's down payment check. • Inspect the customer's check for signs of alteration or forgery. For example, the name and address on the check may appear to be typed rather than printed or may be in a font that is inconsistent with the rest of the check.
Response Procedures
1. Use the American Bankers Association (ABA) online tool for verifying routing numbers: https://routingnumber.aba.com/default1.aspx 2. Call the issuing bank to verify the account. 3. Require that the customer provide a down payment check that reflects his/her actual name and review the check for signs of alteration or forgery. 4. If available, guarantee the check through your dealer's preferred check guarantee company. 5. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 6. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #10
Customer's driver license or other form of identification is hole-punched, expired, or presented in a non-hard copy format (e.g., email, picture, or photocopy).
Detection Methods

Check the expiration date of the customer's current driver license or other government issued photo identification. Physically inspect the license and ensure there is no hole-punched or other markings that would indicate the license has been invalidated.

Response Procedures

1. Do not proceed with the transaction unless the customer physically provides their original government-issued identification (e.g. not a photocopy)
2. Inspect the identification for signs of alteration and forgery.
3. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system.

Red Flag #11

Personal identifying information provided is inconsistent when compared against external information sources used by the dealership, for example, (1) the social security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File or (2) the date of birth provided by the customer in the credit application is substantially different from the date of birth listed in the consumer report (3) SSN no match to name or address.

Detection Methods

When obtaining a consumer report, be alert for warnings and notifications concerning a mismatch between data supplied by the customer and data available to the credit reporting agency, for example:

- Social Security number not issued
- Hit to death master file
- Inquiry SSN format is invalid
- High probability SSN belongs to another
- Match to full name only
- Match to address only
- Date of birth-no match

Response Procedures

1. If the alert describes an issue with the customer's Social Security number, obtain, inspect, and make a copy of the customer's Social Security card.
2. Require that the customer provides identifying documentation that resolves the discrepancy reported by the credit bureau.
3. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.

4. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #12
Identifying information provided by the customer is associated with known fraudulent activity as indicated in alerts or warnings in the credit report or red flag summary.
Detection Methods
Review the consumer's credit report for alerts or warnings that indicate that the customer may be associated with fraudulent activity, for example: • Customer's [SSN, phone number, address] reported as used in true name credit fraud. Note that a true name credit fraud alert occurs when the address, SSN, or phone number provided by the customer matches an address, SSN, or phone number that has been used to commit true name identity theft or credit fraud. "True name" identity theft occurs when someone uses the legitimate name and other identifying information of someone else to commit fraud.
Response Procedures
1. Ask the customer if he/she has ever been a victim of identity theft or had his/her personal information used to commit fraud. 2. If the consumer claims to be the victim of identity theft, ask for proof, such as a copy of a police report. 3. Request documentation that verifies the information provided by the customer on the credit application (e.g., second form of identification, proof of residence, copy of SSN card, employment information, etc.) 4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #13
Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated in alerts or warnings received by the dealership from a credit reporting agency, for example, (1) the address on an application is fictitious, a mail drop, or prison, or (2) the phone number is invalid, or is associated with a paper or answering service.
Detection Methods

Review the consumer report for warnings, notifications, or alerts concerning potential fraudulent activity. For example, the alert may state that the address or phone number belongs to a prison, hospital/clinic, institution, post office, government building, camp site, credit correction service, restaurant/bar/nightclub, storage facility, airport, truck stop, etc.

Response Procedures

1. Use Google, or any other reputable search engine, to verify if the phone number or address indeed belongs to one of the high-risk address types mentioned above.
2. Compare the address used by the customer, as well as previous addresses listed in the consumer credit report, with (1) other documents provided by the customer, such as driver license, vehicle title, personal check, etc. and (2) previous customer account records, if any.
3. Request proof of residence from the customer (either utility bill, mortgage statement, or property tax bill).
4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.
5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #14

The SSN provided is the same as that submitted by other persons opening an account or other customers.

Detection Methods

Review the consumer report for alerts such as:

- Multiple SSNs on file
- Multiple Valid SSNs on File
- SSN associated with additional subjects
- SSN belongs to another

Response Procedures

1. Ensure that you entered the customer's SSN correctly.
2. Request a copy of the customer's SSN card and ensure that the name on the card matches the customer's government-issued ID and name provided in the application.
3. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.
4. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #15
The customer fails to provide all required personal identifying information on an application, is uncooperative in providing personally identifiable information, does not want his/her credit pulled, or refuses to answer out-of-wallet questions.
Detection Methods
Review the customer's credit application and ensure that no required fields are left blank or illegible. Be aware of other suspicions or uncooperative behavior.
Response Procedures
1. Ask the customer for an explanation of why he or she does not want to provide the identifying information. 2. If the customer does not want his or her credit pulled, generate a stand-alone red flag report. 3. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 4. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #16
The customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report (i.e., the customer fails an out-of-wallet quiz).
Detection Methods
Customer fails out-of-wallet question quiz.
Response Procedures
1. Request documentation that verifies the information provided by the customer on the credit application (e.g., second form of identification, proof of residence, copy of SSN card, employment information, etc.) 2. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #17
A co-buyer or co-lessee is included in the vehicle credit sale or lease but is not present at the dealership to sign the contract or lease.
Detection Methods
Be alert of any transaction where the co-buyer or co-lessee is not present or any effort by the customer to request or steer the transaction toward having the co-buyer or co-lessee sign documents off-site.
Response Procedures
1. Advise all relevant employees, as well as the customer, that all paperwork, credit report, and identification procedures used by the dealership for both buyers and co-buyers apply to all transactions. 2. Do not proceed with the transaction if the customer directly or indirectly seeks to avoid compliance with all identity verification procedures. 3. Follow all of the same Red Flag procedures listed in this ITPP for the co-buyer or co-lessee.

Red Flag #18
Customer provides local residence and work address but presents an out-of- state driver license or other government issued ID.
Detection Methods
Be alert of any customer who presents an out-of-state driver license or other government issued ID.
Response Procedures
1. Ensure that the out-of-state driver license is valid and not expired. 2. Review the customer's credit report and see if one of the customer's previous addresses matches the out-of-state ID being presented. 3. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system. 4. Do not proceed with the transaction unless a reasonable and verified explanation that is not indicative of identity theft explains the discrepancy and is documented in the deal file. 5. If available, generate out-of-wallet questions and ensure that the customer receives a passing score.

6. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #19
A customer seeks to execute a vehicle credit sale or lease and take delivery of the vehicle off-site at a location other than the dealership's facility.
Detection Methods
Be alert of any transaction where the buyer is not present or any effort by the customer to request or steer the transaction towards having the documents signed off-site.
Response Procedures
1. If the vehicle must be delivered off site, and the decision to do so is approved by a manager, ensure that you contact your overnight mailing service provider and request that re-routes (or re-directs) are not permitted. 2. Require that any off-site delivery take place at the customer's verified residential address that matches the contract and credit application. 3. Require notarization and an adult signature on the document package you send out. 4. Ensure the bill of lading specifies that re-routes are prohibited. Specifically note in your transport contract that you are to be notified if the driver is asked to change delivery locations. 5. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system.

Red Flag #20
Customer claims to be a referral from a prior customer or dealership employee in order to avoid (1) explaining suspicious activity and identified red flags or (2) providing identifying information.
Detection Methods
Be alert of any customer who claims to be a referral from a prior customer or dealership employee in order to get around explaining red flags or providing identifying information.
Response Procedures

1. Advise all relevant employees, as well as the customer, that all paperwork, credit report, and identification procedures used by the dealership for both buyers and co-buyers apply to all transactions, regardless of whether or not the customer is a referral.
2. Unless approved by the Program Administrator(s) or other senior management, do not make exceptions to the ITPP simply because a customer is a referral.
3. Do not open the account if the customer directly or indirectly seeks to avoid compliance with all identity verification procedures.

Red Flag #21
Customer asks that the contract, lease, or title paperwork reflect an address other than the addresses shown on identification documents or the consumer report.
Detection Methods
Be alert of any customer who asks that the contract, lease, or title paperwork reflect an address other than the addresses shown on identification documents or the consumer Report. Identity thieves will often attempt to have the contract reflect a fictitious or non-residential address as to prevent anyone from detecting the fraudulent account.
Response Procedures
1. Use Google, or any other reputable search engine, to ensure that the address does not belong to a high-risk address type. 2. Request proof of residence from the customer (either utility bill, mortgage statement, or property tax bill). 3. Do not proceed with the transaction until it has been verified that the address provided by the customer is indeed that customer's current residential address. 4. If available, generate out-of-wallet questions and ensure that the customer receives a passing score. 5. Do not proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #22
Customer is impatient, seems to be in a hurry, pressures dealership personnel to rush through the sales/lease process, or seems unusually disinterested in the price and financing of the vehicle.
Detection Methods

Take note of a customer who is impatient, seems to be in a hurry, pressures dealership personnel to rush through the sales/lease process, or seems unusually disinterested in the price and financing of the vehicle.

Response Procedures

1. Unless approved by the Program Administrator(s) or other senior management, do not make exceptions to the ITPP simply because of customer pressure.

Red Flag #23

The length of residence and/or employment information provided by the customer on the credit application is geographically inconsistent or impossible. For example, the customer states he or she has only lived in California for the past 4 years, but shows 2 years of previous employment while living in Missouri during that same time period.

Detection Methods

Review each consumer credit application to identify any suspicious patterns or inconsistencies in employment and residency information.

Response Procedures

1. If available, run the customer's government-issued identification through a counterfeit ID scanner or detection system.
2. If available, generate out-of-wallet questions and ensure the customer receives a passing score.
3. Ask the customer for an explanation of the inconsistency.
4. Compare the address used by the customer, as well as previous addresses listed in the consumer credit report, with: (1) other documents provided by the customer, such as driver license, vehicle title, personal check, etc., or (2) previous customer account records, if any, in your CRM and DMS.
5. If necessary, request proof of residence from the customer (either utility bill, mortgage statement, or property tax bill).
6. Do not open proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

Red Flag #24

A consumer is applying for credit under a business or entity that was just recently formed or incorporated and/or has little to no reputable online presence.

Detection Methods

Check the credit application and contract to see whether the consumer is applying under their personal name or a business/entity name.
Response Procedures
1. Confirm whether the business is a legitimate entity by searching your state's online directory of registered entities, which is normally available through a Secretary of State business search. 2. Determine whether the business has any online presence, such as an active website, Yelp reviews, social media pages, etc. 3. Confirm that the consumer actually holds the title claimed (e.g. Owner/CEO) by checking LinkedIn or publicly available business filing documents. 4. Do proceed with the transaction or submit the application for financing until you have verified with reasonable certainty that the account is not the result of identity theft.

6. Service Provider Oversight

Marchese Ford of Mechanicville will oversee each of its service providers that participate in the opening or maintaining of a covered account, or any other duty covered under this ITPP, to ensure that the service provider has appropriate policies and procedures in place to perform these functions and has agreed to do so contractually.

7. Training

All relevant Marchese Ford of Mechanicville personnel shall receive training, as necessary, to effectively implement and maintain this ITPP. This includes the following:

- Making available a copy of this ITPP to all employees having duties that may involve opening covered accounts or obtaining/viewing consumer credit reports;
- Training all new employees having duties that will involve opening covered accounts or obtaining/viewing consumer credit reports; and
- Training on a recurring, periodic basis, to communicate changes and updates to the ITPP.

8. Enforcement

Violations of this ITPP may result in disciplinary action, up to and including termination, in accordance with Marchese Ford of Mechanicville's human resources policies.

9. Effective Date & Approval of ITPP

This ITPP is effective as of Jun 22, 2022.