Table of Contents

1.0 Purpose

The purpose of these Third Party Requirements ("Requirements") is to provide the minimum expectations Ally and Ally Affiliate Third Parties are accountable to adhere to while performing Services in accordance with the Agreement.

2.0 Scope

These Requirements apply to all Ally Third Parties, as well as their Subcontractors, and should be read in conjunction with the Agreement, as these Requirements are in addition to any obligations or other requirements specified in the Agreement. In the event of any conflict between such obligations or requirements and these Requirements, whichever is most protective of Ally Data shall apply.

3.0 Third Party Requirements

While providing goods or Services to Ally, Third Parties must comply with these Requirements as appropriate without charging Ally any additional fees.

4.0 Definitions

The following definitions apply only to these Requirements. Capitalized terms used but not defined herein have the meanings given to them in the Agreement.

"**Ally Data**" - All data and information that Ally, any Affiliate of Ally or any Ally Third Party provides to Third Party or that otherwise comes into Third Party's or a Third Party agent's possession pursuant to the Agreement. Ally Data includes Consumer Information and Confidential Information of Ally, Ally Affiliates, and Ally Third Parties.

"**Ally Systems**" - Information systems, such as hardware, software, networks, data, tool kits, or other information system resources, owned or licensed by or on behalf of Ally, an Ally Affiliate, or an Ally Third Party, that may be used or accessed by Third Party or is integrated with Third Party IT Systems in connection with the Services, in each case, excluding the Third Party's own IT Systems.

"**Artificial Intelligence (AI)**" - The application of computational tools to address tasks traditionally requiring human intelligence.

"**Computing Asset**" - Any technology asset including, but not limited to, personal computers, laptops, and Virtual Machines, used in support of Ally operations. A Virtual Machine is a software emulation of a physical computing environment.

"**Controls Effectiveness Review (CER)**" – Due diligence performed on a Third Party to determine the effectiveness of their control environment as it relates to the service provided to Ally. CERs are performed as necessary based on the risk level of the Third Party or the service provided. After the initial CER is completed, update CERs are completed based on risk or service change triggers.

"**Electronic Physical Access Control System**" - A method of securing entrances and exits to sensitive areas of Third Party's business that is administered by a computer program and provides end users with a means of access that is trackable to the individual user, to include time, date, entry point, and action of the system.

"**High-Security Area (HSA)**" - A specific area within a Third Party location where an additional layer of security (restricted access) is required due to the large amounts of sensitive data, value of physical assets and work performed in the area (e.g., data centers, vaults, UPS rooms, etc.).

"**IT System**" - Any collection of computing and/or communications components and other resources that support one or more of Third Party's functional objectives. IT System resources include all electronic data processing, information, recordkeeping, communications, telecommunications, account management, inventory management and other computer systems used in the acquisition, storage, manipulation, display, and/or movement of data or to direct or monitor operating systems. An IT System may consist of one or more computers and their related resources of any size. The resources that comprise an IT System do not have to be physically connected.

"**Non-Public Ally Data**" - All Ally Data, including Proprietary, Confidential, and Secret Ally Data that has not been explicitly approved by Ally management for general release to the public. All Ally Data is classified as follows, in order of lowest to highest restriction level:

Public: Ally Data that has been explicitly approved by Ally Management for general release to the public.

Proprietary: All Non-Public Ally Data that, if lost or unavailable, disclosed to unauthorized individuals, or inappropriately altered, would have a low or limited impact on Ally Proprietary is the default classification for all Ally Data, and Ally Data classified as such is generally available to authorized users and clients during the course of conducting business.

Confidential: All Non-Public Ally Data that, if lost or unavailable, disclosed to unauthorized individuals, or inappropriately altered, could cause substantial harm to Ally customers, clients, or employees, violation of legal or regulatory requirements, or financial penalties or reputational damage to Ally. The protection of Ally Data classified as Confidential requires control measures beyond those required for Proprietary information, and access to Ally Data classified as such is restricted to a defined group of individuals or entities. Ally Data classified as Confidential includes Personally Identifiable Information (PII), Payment Card Industry Data (PCI) and Protected Health Information (PHI).

Secret: All Non-Public Ally Data that, if lost or unavailable, disclosed to unauthorized individuals, or inappropriately altered, could compromise a strategic business initiative, and cause substantial damage to the competitive position of Ally or any Ally business's product line or financial position, or pose a significant operational, information security, business, or strategic risk. Secret is the most restrictive classification for Ally Data, and Ally Data classified as such is restricted to select individuals with explicit authorization from Ally Management. For the avoidance of doubt, Non-Public Ally Data that is not PII is

"Confidential Information" of Ally as used in the Agreement, Non-Public Ally Data that is PII is "Consumer Information" as used in the Agreement.

"**Payment Card Industry Data (PCI)**" - Refers to cardholder data and/or sensitive authentication data, including the following:

- Cardholder Data:
  - Primary account number (PAN)
  - Cardholder name
  - Service code
  - Expiration date
- Sensitive Authentication Data:
  - Full track data (data from the magnetic stripe, equivalent data on the chip, or elsewhere)
  - CAV2/CVC2/CVV2/CID (the three-or four-digit value printed on the front or
  - back of a payment card)
  - PIN/PIN Block (personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message).

"**Personal Information or Personally Identifiable Information (PII)**" - Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

"**Privacy Event**" - Any suspected, potential, or confirmed, unauthorized access to or use of Personal Information that Ally maintains; or any suspected, potential, or confirmed disclosure of Personal Information that Ally maintains to an unauthorized party.

"**Protected Health Information (PHI)**" - Information, including demographic information, which relates to:

- the individual's past, present, or future physical or mental health or condition
- the provision of health care to the individual
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify that individual.

"**Regulated Third Party**" - Third Party who operates under the supervision and is subject to the rules and regulations of regulatory authorities with regard to the service(s) provided to Ally.

"**Regulated Work**" - Refers to services the Third Party is providing to Ally or on Ally's behalf which are subject to the rules and regulations of regulatory authorities.

"**Subcontractor**" - A person or entity, other than Ally and the entity named as "Third Party" in the Agreement preamble that has been delegated or assigned certain performance obligations that may involve access to Ally site's, Ally System(s) or Ally Data under the Agreement.

"**Third Party**" - An entity that has entered into a business arrangement with Ally to provide goods or services.

"**Visitor**" - Individuals visiting Third Party's site who are not employees or contractors performing work on a regular basis for Third Party. (e.g., vendors making deliveries, individuals applying or interviewing for a job, family or friends of employees or contractors and anyone who does not have regular authorized need for physical access)

5.0 Anti-Fraud & Conduct Risk Management

As described below and elsewhere within these Requirements, Third Parties are expected to adhere to guidelines for effective management and monitoring of potential unethical behavior, including fraud, bribery, corruption, dishonesty, and money laundering.

5.1 Ally requires Third Parties to comply with all Applicable Laws with respect to unethical behavior.

5.2 Ally requires Third Parties to document and communicate a zero-tolerance expectation for willful or negligent misconduct through a personal responsibility message defining and prohibiting unethical behavior to all employees and subcontractors (i.e., Code of Conduct, Employee Handbook).

5.2.1. Ally requires Third Parties to maintain records evidencing the annual review and attestation of the personal responsibility message defining and prohibiting unethical behavior by all employees and Subcontractors.

5.3 Ally requires Third Parties have a method for detecting internal fraud/unethical behavior (i.e., fraud controls).

5.4 Ally requires Third Parties to communicate clear expectations for reporting instances of unethical behavior to Third Party employees and Subcontractors.

5.5 Ally requires Third Parties to provide Third Party employees and Subcontractors with an anonymous method for reporting unethical behavior.

5.6 Ally requires Third Parties to document their whistleblower and/or anti-retaliation protections for individuals who, in good faith, report instances of unethical behavior.

5.7 Third Parties must report to Ally, any illegal, unethical, or improper behavior or incidents they observe or which they become aware of that pertains to Ally.

5.8 Third Parties can report these instances by:

- Calling the Ally Ethics Hotline (U.S. and Canada) at 800-971-6037
- A secure webpage at: www.allyethics.com
- Email to Ally's Enterprise Fraud, Security, & Investigations (EFSI) team at: SecurityOperationCenter@ally.com
- Contacting Ally's Legal Staff
- Phone or email to any member of EFSI.

5.9 Ally requires Third Parties to have a documented and communicated method for detecting, disclosing, and managing any situations in which an employee, subcontractor or agent has competing interests or loyalties because of duties to one or more organizations (i.e., Conflict of Interest program).

6.0 Domestic Background Check Requirements

Background Check Requirements Table

Requirement	Supplier Type A	Supplier Type B	Supplier Type C	Supplier Type D
Criminal Background	Min. 10 Year	Min. 7 Year	Min. 7 Year	Min. 7 Year
Credit Check	Applies	Applies		
Motor Vehicle Record			Applies	
Sex Offender	Applies	Applies	Applies	Applies
OFAC/Global Sanctions	Applies	Applies		
SSN Tracing	Applies	Applies	Applies	Applies

Third Party Type A: Third Parties who have direct contact with Ally deposits consumers on Ally's behalf and who have the ability to manipulate, transact, process, or review Ally customer account transactions. Third Parties are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.6).
Third Party Type B: Third Parties who have direct contact with Ally consumers (excluding deposit consumers) on Ally's behalf, and having the ability to manipulate, transact, process, or review Ally customer account transactions, and/or contractors/staff augmentation providers with access to Ally sites and/or systems with access to any level of Ally secret, confidential, and/or proprietary information thru means of an Ally Z-ID, email, or Ally systems access. Parties are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.6).
Third Party Type C: Third Parties operating motor vehicles in the delivery of services to Ally. Third Parties are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.6).
Third Party Type D: All other Third Parties receiving Non-Public Ally Data. Third Parties are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.6).
Third Party Type E: All other Third Parties not receiving Ally Data. – No requirements.

6.1 Requirements

6.1.1. Third Party will conduct background checks as set forth in Ally's "Domestic Background Check Adjudication Criteria" (section 6.6) based on application of the Background Check Requirements Table in section 6.0. Where applicable and except when expressly prevented by local laws and regulations, the Third Party will conduct background checks consistent with these Requirements for the purpose of:

6.1.1.1. Verifying the accuracy of information provided by Third Party employees or Subcontractors and their employment eligibility prior to hire and during a Third Party employee's or Subcontractor's course of employment ensuring the ongoing eligibility to view and access Ally data; and

6.1.1.2. Maintaining compliance with any applicable regulatory requirements for more in-depth checks.

6.1.2. Upon request by Ally, Third Party will promptly furnish copies of its background check processes and procedures.

6.1.3. Upon request by Ally, Third Party will provide evidence of specific background check findings and that it has adhered to these background check requirements.

6.2 Criminal Background Check Finding

6.2.1. Third Party must verify prior to Services commencing that Third Party employees and

Subcontractors have been screened for criminal records as set forth in Ally's "Domestic Background Check Adjudication Criteria" (section 6.6) based on application of the Background Check Requirements Table in section 6.0.

6.2.2. Screens should include Federal, National, State and County searches for criminal records (including convictions) based on residential address history for any felonies or misdemeanors as guided by the "Domestic Background Check Adjudication Criteria".

6.2.3. Third Party must disclose to Ally within five (5) business days any existing Third Party employee(s) or Subcontractor(s) that incur any misdemeanor and felony criminal convictions, pretrial diversions, deferred adjudication, or similar programs.

6.3 Credit Background Check Finding (if applicable based on Third Party Type)

6.3.1. Third Party must screen Third Party employees' and Subcontractors' credit reports set forth in Ally's Domestic Background Check Adjudication Criteria prior to providing Services to Ally.

6.3.2. Third Party must verify that Third Party employees' credit reports have no items in Collections, liens, judgments, accounts charged to profit/loss, repossessions or one or more accounts reporting 90 days or more past due that in the aggregate totals more than $50,000.00 prior to providing Services to Ally.

6.3.3. Mortgage roles only – Prior to Third Party employees or subcontractors taking Ally Mortgage roles, Ally requires that the Third Party validates that Third Party employees' and subcontractors' credit reports have no items in collections, liens, judgments, accounts charged to profit/loss, repossessions or one or more accounts reporting 90 days or more past due that, in the aggregate, totals more than $10,000.00.

6.4 Motor Vehicle Record Background Check Finding (if applicable based on Third Party Type)

6.4.1. As set forth in Ally's Domestic Background Check Adjudication Criteria, Third Party must validate that the Third Party employee's or Subcontractor's current license is in good standing and not suspended, revoked, expired, or has 7 or more points based on the ARI Point System.

6.5 Additional Checks set forth in Ally's Domestic Background Check Adjudication Criteria (if applicable based on Third Party Type)

6.5.1. **Sex Offender Registry**

Third Party must search the National Sex Offender Registry and determine no matches for a registered offender. Potential risk should be assessed. Decisions must not be based solely on records in the state criminal database searches. Consider reportable sex conviction(s).

6.5.2. **Global Sanctions**

Third Party validates no hits, including OFAC hits, General Services Administration (GSA) hits and FDIC enforcement actions.

6.5.3. **SSN Tracing**

Third Party validates SSN matches Third Party employee or Subcontractor through background, credit, or similar verification database. Visual inspection of documents alone is not sufficient.

6.6 Ally Domestic Background Check Adjudication Criteria

Applicable to: Third Party Types A, B, C, and D

Purpose: To define requirements of Ally Financial for specific types of background checks to be performed by Third Party prior to hiring applicant(s) in support of activities related to Ally Financial.

Requirements: Where applicable and except when expressly prevented by local laws and regulations,

Third Party will conduct background checks consistent with the requirements identified within the Ally Third Party Requirements. The Third Party is responsible to determine applicants' final disposition after the applicable background checks and adjudications are conducted.

DESCRIPTION	DISPOSITION
Hiring process continues. Background screening results do not contain any potentially adverse information and no questions arise from answers to adjudication criteria.	Pass
The applicant's background screening results have triggered questions that require additional review prior to changing status to a Pass or Fail and initiating the FCRA process. Adjudicator reviews all available information and may request letter of explanation and specific documentation (i.e., court documents, incident/police report, etc.).	Review
The applicant's background screening results have triggered the defined adjudication criteria and the hiring process for the candidate stops. An individualized assessment is performed for any finding triggering the adjudication criteria prior to final decision. If the assessment/Review does not mitigate result/s, the FCRA pre-adverse letter is sent via e-mail to the address on file. This is followed by the adverse letter after 5 business days if the applicant does not dispute the decision, or if the information provided by the applicant does not change the decision.	Fail
Background screening vendor has submitted all necessary requests to verify all information provided on the applicant's employment application. However, some requests may need additional time.	Pending

Note:
Candidates who initially fail the credit component(s) are eligible for re-hire after a 6-month waiting period from the date the Adverse Letter is sent.

Canadian Residents (The nonimmigrant NAFTA Professional (TN) visa)
Candidates who reside in Canada but have a TN and cross the border each day, should be reviewed under U.S. screening standards, including FCRA and individual state laws.
Candidates who reside in Canada and work from home in Canada should be screened under Canadian law including applicable Canadian federal privacy and human rights laws, and specific provincial laws.

FDIC 19 GOVERNED CRIMINAL OFFENSES COMPONENT

CRIMINAL BACKGROUND CHECK FINDING

Section 19 of the Federal Deposit Insurance Act (12 U.S.C. 1829) governs whether an individual may be employed by a federally insured depository institution (Bank). Section 19 prohibits, without the prior written consent of the Federal Deposit Insurance Corporation (FDIC), a person convicted of any criminal offense involving dishonesty or breach of trust or money laundering (covered offenses), or who has agreed to enter into a pretrial diversion or similar program (program entry) in connection with a prosecution for such offense, from becoming or continuing as an institution-affiliated party, owning or controlling, directly or indirectly an insured depository institution insured institution), or otherwise participating, directly or indirectly, in the conduct of the affairs of the insured institution. In addition, the law forbids an insured institution from permitting such a person to engage in any conduct or to continue any relationship prohibited by Section 19. It imposes a ten-year ban against the FDIC's consent for persons convicted of

certain crimes enumerated in Title 18 of the United States Code, absent a motion by the FDIC and court approval. De minimis exceptions: Approval is automatically granted, and an application will not be required where all of the following de minimis criteria are met. 1) The individual has been convicted of, or has program entries for, no more than two covered offenses, including those subject to paragraph (b) of this section; and for each covered offense, all of the sentencing requirements associated with the conviction, or conditions imposed by the program entry, have been completed (the sentence- or program-completion requirement does not apply under paragraphs (b)(2) which covers bad checks and (b)(4) which covers fake or false identification; 2) Each covered offense was punishable by imprisonment for a term of one year or less and/or a fine of $2,500 or less, and the individual served three days or less of jail time for each covered offense; 3) If there are two convictions or program entries for a covered offense, each conviction or program entry was entered at least three years prior to the date an application would otherwise be required, except as provided in paragraph (b)(1) which covers the 18 month waiting period when 21 years old or younger; and 4) Each covered offense was not committed against an IDI or insured credit union. **FDIC HIGHLIGHTS**: • Industry applications for employment, background check programs, and hiring practices must comply with Section 19. Offenses covered by Section 19 have no statute of limitations. Therefore, institutions must consider a job applicant's entire legal history. • In matters related to Section 19, federal law pre-empts applicable state law(s). Ally recognizes, however, that some state / local jurisdictions have limited reporting timeframes for criminal history (e.g., 7 years). If a Third Party candidate(s) reside in these states / localities and the Third Party is unable to access criminal reporting for a candidate(s) due to a state / local reporting limitation, Ally will deem the Third Party to have satisfied the criminal history search so long as the Third Party has completed the search for the maximum period permitted by the state / local jurisdiction. A position statement, police reports, and final disposition may be required for candidates who fall under 'review' for the criminal component. Criminal background findings for residents or candidates residing or employed in Massachusetts is limited to 3 years.	**DISPOSITION**
Criminal conviction for any felony or misdemeanor involving theft, fraud, burglary, forgery, robbery, embezzlement, dishonesty or breach of trust, money laundering, misappropriation crimes without regard to the date of conviction.	Fail
Criminal conviction for misdemeanor offenses older than 10 years and not involving any of the above-listed offenses under the purview of FDIC Section 19 where there is no similar conduct or pattern since the conviction.	Review

All convictions or program entries for offenses concerning the illegal manufacture, sale, distribution of, or trafficking, in controlled substances will require an application with the FDIC unless they fall within the provisions for de minimis offense set out in FDIC Section 19.	Fail
No record found (includes expunged or sealed records).	Pass
Criminal conviction or program entry for small dollar, simple theft of goods or services (excludes burglary, forgery, robbery, identity theft, and fraud) which total $1,000.00 or less at time of conviction or program entry and theft did not involve a financial institution or insured credit union. If more than one de minimis offense, must also consider de minimis exception section above. Note: $500.00 or less is considered a misdemeanor in most states except Florida, where it is a felony if value is greater than $300.00, and New Jersey where $200.00 is considered a felony. Ally defers to FDIC guidance therefore the $500 threshold applies.	Pass
If there are no more than two criminal convictions or program entries for a covered offense, and the actions that resulted in both convictions or program entries all occurred when the individual was 21 years of age or younger, the convictions or program entries/ sentencing requirements have been completed, and at least 18 months have passed.	Pass
Multiple criminal convictions for bad or insufficient funds checks if the total of all checks across all convictions $1,000.00 or less. May be considered a pass unless the payee is a financial institution or credit union.	Pass
Criminal conviction for use, creation, or possession of a fake or altered ID card by a person under the age of 21 to circumvent age-based restrictions to obtain or purchase alcohol or commit any other crimes related to purchases, activities, or premises entry by someone under the legal age if there is no other conviction.	Pass
Any pretrial diversion, deferred adjudication, or similar program. (The FDIC regulations explicitly state that a pre-trial diversion, similar to an adjudication withheld for a crime of dishonesty has the same effect as a conviction).	Review
ALLY BACKGROUND CHECK COMPONENTS **CRIMINAL BACKGROUND CHECK FINDING**	**Disposition**
Criminal conviction for any felony involving violence, sex crimes, cyber-crimes, bullying, stalking, terrorism, illegal possession of weapons, illegal drugs (except marijuana possession offenses not governed by the FDIC), or any misconduct related convictions in the last 7 years. Criminal conviction for any of the above listed felony offenses older than 7 years where there is no similar conduct or pattern since the conviction.	Fail Review
Criminal conviction for any misdemeanor involving violence, sex crimes, cyber-crimes, bullying, stalking, terrorism, illegal possession of weapons, illegal drugs (except marijuana possession) or any related convictions in the last 7 years. Criminal conviction for any of the above listed misdemeanor offenses older than 7 years where there is no similar conduct or pattern since the conviction.	Fail Pass

Criminal conviction for any traffic or vehicle code violation that does not fall into another category above.	Pass
Driving while under the influence or related conviction (one conviction/infraction only). DUI offenses older than 7 years.	Pass
Driving while under the influence or related conviction (more than one conviction). Review pattern and determine if potential conflict. If three or more convictions reported in the last 3 years or felony level, would result in fail if responsibilities involve driving.	Review
CREDIT BACKGROUND CHECK FINDING	**DISPOSITION**
If credit report has no items in collections, liens, judgments, accounts charged to profit/loss, repossessions or one or more accounts reporting 90 days or more past due, that in the aggregate total more than $50,000.00.	Pass
Note: For individualized assessment, applicant may provide a letter of explanation and supporting documentation if credit findings fall outside of established criteria prior to further review.	Fail
SOCIAL SECURITY NUMBER TRACE	**DISPOSITION**
SSN matches candidate name.	Pass
SSN matches candidate name PLUS another name.	Pass
SSN no record identified (meaning no credit reported for the applicant's SSN).	Pass
SSN matches name OTHER THAN candidate name.	Review
SSN not yet issued.	Review
MVR BACKGROUND CHECK FINDING	**DISPOSITION**
Current license suspended, revoked, or expired.	Fail
Review and assign points according to ARI Point System. Candidate Score > or = 7	Fail
Review and assign points according to ARI Point System. Candidate Score <7	Pass
ADDITIONAL CHECKS	**DISPOSITION**
Sex Offender Registry - Search matches registered offender (Potential risk should be assessed). Note: Decisions must not be based solely on records in the state criminal database searches of the sex offender registry. Consider reportable sex conviction.	Fail Review
Global Sanctions (which includes OFAC hits, General Services Administration (GSA) hits and FDIC enforcement actions) - Any Hit.	Fail

RECONSIDERATION AFTER FAILED BACKGROUND COMPONENT	TIME PERIOD	NOTES

Credit	6 months	Must review full background
Criminal	6 months	Must review full background. Conviction causing fail must have been expunged or dismissed and no other relevant criminal convictions since prior adjudication.

7.0 Equal Opportunity Employment

Third Party will comply with all applicable laws and regulations related to fair employment. Ally expects Third Parties performing Services for Ally to value the wide range of backgrounds of Third Party's employees and strive to create work environments that reasonably accept and embrace differences while promoting productivity and teamwork. Diversity and inclusion should be key components of Third Party's and Subcontractors' core values and contribute to a healthy and engaging culture. All Third Parties are responsible for creating and maintaining a productive work environment where the dignity of all individuals is respected. Third Parties should also treat customers, vendors, and guests, as well as the public in general fairly and with respect. Third Party shall not tolerate unlawful discrimination of any kind in any of its employment or business practices.

7.1 Employment Standards

7.1.1. Third Party will ensure that each individual, performing Services under the Agreement has the right to work in an atmosphere that promotes equal opportunities and prohibits unlawful discriminatory practices, including harassment and discrimination based on age, race, color, sex, religion, national origin, disability, sexual orientation, gender identity or expression, pregnancy status, marital status, military or veteran status, genetic disposition or any other status protected by law. These standards apply to Third Parties at all locations where Ally business is conducted and other non-company locations if the conduct affects the work relationship.

7.1.1.1. Harassment is pervasive unwelcome and/or hostile verbal, physical or visual conduct toward an individual because of age, race, color, sex, religion, national origin, disability, sexual orientation, gender identity or expression, pregnancy status, marital status, veteran status, genetic disposition, or any other status protected by law when the conduct creates an intimidating, hostile or offensive work environment; causes work performance to suffer; or negatively affects job opportunities. Specific actions that can be considered harassment include, but are not limited to, verbal conduct including offensive name calling, jokes, slurs, negative stereotyping and threatening, intimidating or hostile acts; non-verbal conduct such as staring, leering, and giving inappropriate gifts; physical conduct such as assault, unwanted touching, intentionally blocking normal movement and interfering with work; and visual conduct such as derogatory posters and offensive photography, cartoons, drawings and gestures. Inappropriate email or internet content in the workplace may also be harassment.

7.1.1.2. Discrimination occurs when work-related decisions (e.g., hiring, firing, compensation, the terms and conditions or privileges of employment) are based on factors such as age, race, color, sex, religion, national origin, disability, sexual orientation, gender identity or expression, pregnancy status, marital status, veteran status, genetic disposition, or any other status protected by law.

7.2 Accountability and Monitoring

7.2.1. If, while performing Services under the Agreement, a Third Party individual feels he or she is being harassed or discriminated against, or observes harassment or inappropriate behavior, he or she should advise the person engaging in the inappropriate or improper behavior that the behavior is inappropriate or improper and should be stopped. If the individual is uncomfortable in directly dealing with the person engaged in the behavior or the person does not respect the request to stop, the individual should report the behavior to an appropriate Third Party supervisor or department. The Ally Ethics Hotline may also be accessed if the behavior involves Ally or an Ally employee.

7.2.2. It is the responsibility of every Third Party individual to report to Ally any alleged discrimination or harassment witnessed or experienced while performing services to Ally. Allegations of harassment and discrimination should be promptly investigated. Retaliation

against anyone who reports a suspected violation of these Requirements or who cooperates in the investigation of an alleged violation should not be tolerated. Third Party should take disciplinary action, up to and including termination of the employment or business relationship, in response to a violation of any of these requirements. Any individual who believes that there has been a violation of these requirements must immediately report the violation to their management, their Human Resources department, or their internal ethics office or hotline. To the extent a Third Party's employee witnesses any violations or potential violations to these requirements involving Ally or on Ally premises, Third Party should report such violation or potential violation to the Ally Ethics Hotline.

8.0 Information Security Standard Requirements

A guaranteed level of information security from our Third Parties is crucial to Ally's business. Ally, as Financial Holding Company, is required under current laws and regulations, to ensure that Ally's Third Parties have implemented adequate information security controls to safeguard Ally business and customer information. Third Parties must meet these stated security requirements or have implemented equivalent or more restrictive controls as reasonably determined by Ally General Information Security Requirements.

8.1 General Information Security Requirements

8.1.1. Third Party's management must develop, approve, and maintain an Information Security Policy based on industry recognized security frameworks that is published and communicated to all employees and relevant external parties. Third Party must ensure an information security awareness campaign is provided to all personnel who accesses Ally information or assets. Third Party must educate personnel of their responsibilities to secure Ally information or assets.

8.1.2. Third Parties must have a documented and followed information security program/policy that is based on industry recognized security frameworks, such as International Organization for Standardization ("ISO") 27001 National Institute of Standards and Technology ("NIST") Special Security Publications.

8.1.3. Third Party must document, implement, and follow rules for the acceptable use of computing assets and must require its assets to be used in a professional, lawful, and ethical manner. Any activities which have been identified as unacceptable are prohibited.

8.1.4. Third Party must define, document, and assign ownership to oversee development, adoption, enforcement and compliance with information security requirements, policies, standards, and procedures.

8.1.5. Third Party must periodically assess risks within its information technology (IT) environment that is used to access, maintain, or support Ally Data or Ally Systems.

8.1.6. Third Party must have a managed and up to date inventory of Third Party's assets that are used to support or access Ally Data or Ally systems including cloud services and functions.

8.1.7. Third Party is required to ensure that their subcontractors are compliant with the requirements in this document. If requested by Ally, Third Party must provide adequate validation that any of its subcontractors are compliant with this document.

8.1.8. All Third Parties who connect to or use an Ally system (including servers, workstations, infrastructure, internet gateway, or network) must abide by all applicable Ally terms of use and any supporting standards and procedures.

8.2 Application and Software Development and Management

8.2.1. Third Party must have a documented Software development life cycle (SDLC) methodology that include version control and release management procedures.

8.2.2. The software development process must contain activities that foster development of secure software (e.g., security requirements in requirements phase, secure architecture design, static code analysis during development, and dynamic scanning or penetration test of code during QA phase, with vulnerabilities identified using those methodologies remediated before moving to the next phase).

8.2.3. Third Party must have, maintain, and follow documented change management procedures. Additionally, Third Parties must notify Ally in advance of each release with potential to impact Ally, including those that may change the existing features, or impact feature functionality, operability, or secure of the Services, or cause the Services to be unavailable.

8.2.4. Third Party must ensure, and confirm to Ally, that any changes to IT systems that are performing work on or for Ally are tested prior to deployment and do not have any negative security implications.

8.2.5. Replacement or risk mitigation strategies must be in place for operating systems, software applications, and critical infrastructure components that are nearing end of life.

8.2.6. Additionally, Third Party must not use software, firmware, hardware, or other systems no longer supported by their vendor when hosting, developing, or maintaining Ally data.

8.3 Data Backups

8.3.1. Third Party must have a defined backup policy and associated procedures for performing backup of Ally data in a scheduled and timely manner.

8.3.2. Third Party must ensure that Ally data is securely transferred or transported to and from backup locations and must conduct periodic tests to ensure that data can be safely recovered from backup devices.

8.3.3. Effective controls must be established to safeguard backup data (onsite, offsite, or cloud).

8.4 Data Protection

8.4.1. All Ally Data classified as Confidential or higher, where permitted by Law, must be subject to data loss prevention (DLP) filtering on any system that is used to develop, support or host Ally data.

8.4.2. All Third Party managed laptops that are used to store, access, support or transmit Non-Public Ally Data must be protected with a full disk encryption solution I

8.4.3. Third Party must not transfer Non-Public Ally Data to a non-production environment.

8.4.4. Information must be classified in accordance with this standard. For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined.

8.4.4.1. **Public information** is information that has been approved by Ally management for general release to the public. Some examples may include:

- Advertising materials
- Company brochures
- Annual reports
- Information displayed on the Ally.com website.

8.4.4.2. **Proprietary information** is the default classification for all Ally information. Proprietary information is any Non-Public Ally information available to authorized users and clients during the normal course of conducting business. Access to Proprietary information is generally unrestricted within Ally. The loss, unauthorized disclosure, or inappropriate alteration of Proprietary information would have a low or limited impact on the company. Some examples may include:

- Internal organization announcements
- Departmental budget information
- Memos
- Governance Documents

8.4.4.3. **Confidential** –. Data classified as “Confidential” is any Non-Public Ally Information, including Personally Identifiable Information (PII), Payment Card Industry Data (PCI) and Protected Health Information (PHI), whose access is restricted to a defined group of individuals defined by the Ally Business Owner. Refer to Appendix I of this Standard for definitions of these protected data categories. The protection of Confidential information requires control measures beyond those required for Proprietary information. The loss, unauthorized disclosure, or alteration of Confidential information could cause substantial harm to Ally customers, clients, or employees, violation of legal or regulatory requirements, or financial penalties or reputational damage to Ally. Each data related interaction containing PII elements should be evaluated on a case-by-case assessment of the specific risk that an individual can be

identified. The term “Sensitive” refers to Confidential or Secret information but is not used as a classification within Ally. Some examples may include:

- Internal organization plans (prior to release)
- PII, PCI, and PHI data elements
- Strategic departmental efforts
- Employee Human Resource information
- Customer financial account information
- Any other personal information as described below
- Audit reports
- Regulatory exam reports

8.4.4.4. **Secret** – information is Non-Public Ally Information that, if disclosed to unauthorized individuals, may compromise a strategic business initiative, and cause substantial damage to the competitive position of a Business Line (e.g., product line or financial position) or to Ally as a whole. Exposure of the data to unauthorized persons will pose a significant Operational, Information Security Risk and/or Business/Strategic Risk. Secret is the most restrictive classification of information and must only be available to select individuals with explicit authorization from Ally Management. Information classified as Secret is often only shared in paper format or on dedicated servers to protect its confidentiality.
Some examples may include:

- Quarterly earnings reports before they are released
- API tokens
- Access tokens
- Authentication credentials
- Passwords or Encryption keys
- Material non-public information
- Strategic contract negotiations
- Nonpublic company merger and acquisition information

8.4.5. If applicable to the services provided to Ally, Third Party must secure all credit card data in accordance with requirements listed in the most current and released editions of the PCI DSS and must annually provide evidence of PCI certification or compliance.

8.4.6. When Ally data is no longer required, it must be deleted or erased, using commercially available tools or methods, in such a manner as to make the data unusable and unretrievable evidence of data destruction must be provided to Ally upon request.

8.4.7. Data destruction processes for hardware and physical media must securely wipe all data on all media using a method that will not allow data to be retrieved, or physically damage the media rendering the information unrecoverable. These processes must be performed in accordance with the National Institute of Standards and Technology Special Publication 800-88 Revision 2, Guidelines for Media Sanitization.

8.5 Encryption

8.5.1. The use of known weak or flawed encryption methods is prohibited.

8.5.2. Secure Key governance must be employed by Third Parties to assure the confidentiality, integrity, and availability of cryptographic key material.

8.5.3. Ally’s minimum standard for cryptographic algorithms and minimum key lengths must be used when implementing encryption:

8.5.3.1. Symmetric Ciphers

- Advanced Encryption Standard (AES), key length of 128, 192, or 256 bits.

8.5.3.2. Asymmetric (Public Key) Ciphers

- Rivest-Shamir-Adleman (RSA)
- Minimum of 2048-bit Keys must be used for all systems.

8.5.3.3. Hashing Algorithms

- Secure Hashing Algorithm (SHA-2 or SHA-3 series), minimum key length of 256 bits

8.5.3.4. Transport Layer Security (TLS) protocol

- TLS v1.2 minimum, for all systems including those subject to compliance with the Payment Card Industry Data Security Standard (PCI DSS)

8.5.4. Secure encrypted transmissions must be used for all Non-Public Ally Data while:

- In transit over any public shared network including the internet.
- In transit over any wireless network.
- In transit to any external source or 4th party.
- Within a Third Party data center unless robust physical and logical controls are in place.

8.5.5 All Ally Data stored by the Supplier that is classified by Ally as Confidential or Secret must be encrypted at all times.

8.6 Identity and Access Management

8.6.1. Third Party must ensure all user IDs, tokens or physical access badges are assigned to a unique employee or subcontractor.

8.6.2. Third Party must use authentication and authorization technologies for service, user, and administrator level accounts.

8.6.3. Third Party must ensure IT administrators are provided and using separate and unique administrator accounts that are only used for administration responsibilities. Non-administration tasks must always be performed using non-administrator user accounts.

8.6.4. Third Party must not allow direct access to the default administrator user accounts such as root or administrator. All systems must prompt users to re-authenticate when users attempt to elevate their privileges to higher security levels. Examples include use of sudo or su on Unix/Linux systems or “run as” for Microsoft Windows based systems.

8.6.5. Third Party must ensure systems that support access to Non-Public Ally Information always requires the following password construction requirements:

- Minimum length: 8 characters
- Complexity: Must contain at least three of the following four characters: number, uppercase letter, lowercase letter, printable special character.
- History (reuse): > 6 passwords
- Expiration: For all end user accounts: passwords must be changed annually.
- For all privileged user accounts: Where a commercial Privileged Access Manager (PAM) tool is used that vaults or rotates the password, no expiration required.
- Where MFA is in place, passwords must be changed annually.
- Where only a user ID/Password are used, passwords must be changed every 180 days.
- Failed login attempts: <= 6 attempts
- Account lockout: Accounts must remain in locked status for a minimum of 30 minutes or until manually unlocked by an administrator, or have a secure self-serve method in place.
- A user’s identity must be verified before a password is reset, and an email or voicemail notification must be sent to notify the user that the password was reset.

- Inactive application user sessions must be shut down after a defined period of inactivity – not to exceed 30 minutes.
    - For systems that are subject to compliance with the PCI DSS, re-authentication is required when a session is idle for more than 15 minutes.

8.6.6. Third Party must ensure that systems used to access Non-Public Ally Information or assets meet the following additional requirements at all times:

8.6.6.1. Authentication credentials must be encrypted when stored or transmitted.

8.6.6.2. Passwords must not be communicated via email messages or other forms of electronic communication, other than one-time use passwords.

8.6.6.3. First-time passwords for new user accounts must be set to unique values that follow the construction requirements and must not be generic, easily guessed passwords.

8.6.6.4. User accounts must be configured to force a change of password upon first use of a new account or after a password is reset.

8.6.6.5. All manufacturer passwords must be changed from the default values (including when the default value is NULL) and must meet or exceed the construction requirements set forth in this standard. Manufacturer passwords include, but are not limited to, SNMP community strings, system-level administrator account passwords, temporary account passwords, wireless encryption keys, and other default authentication settings.

8.6.7. Password fields must display only masked characters as the user types in a password, where technically feasible.

8.6.8. Third Party must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.

8.6.9. Third Party must immediately notify Ally if a Third Parties employee or subcontractor with access to Ally Data or Systems is terminated, or not working on the Ally account. All account permissions must be updated on Third Parties or Ally managed technology to reflect these changes. Notices must include name, user ID, and names of any accounts the person had access to or knows the password.

8.6.10. Third Party must ensure procedures exist for appropriate provisioning, management, and deprovisioning of privileged accounts.

8.6.11. Third Party must periodically review the necessity and assignment of privileged access accounts no less than annually.

8.6.12. If a Third Party requires remote access to Ally data or systems that Third Party must always use an Ally approved method.

8.6.13. The Third-Party Third Party is required, by the commencement date, to provide an authentication process that meets Ally's requirements as set forth within this standard.

8.6.14. If during the term of the agreement, the Third Parties authentication process does not comply with applicable laws or regulations, the Third Party must notify Ally in writing within ten (10) business days and to modify its authentication process within a reasonable time period to comply with requirements within the applicable laws or regulations.

8.6.15. The "authentication process" means the process of authenticating and verifying a customer's identity to ensure they are the proper user to access information concerning the Third Parties product or service via electronic means (including, without limitation, through online access or mobile application). Examples of authentication are username and password validation, multi-factor authentication, and functionality to retrieve credentials such as forgot username/password, as well as mitigating controls such as access attempts and locks, alerts, and unlock functionality by internal associates such as certificate signing requests.

8.6.16. Notwithstanding the foregoing, Ally and the Third-Party Third Party may agree to an alternative solution if such terms and costs are mutually agreed to.

8.7 Monitoring, Response, and Recovery

8.7.1. Third Party must have a documented plan and associated procedures for response to an information security incident. The incident response plan must clearly articulate the

responsibilities of personnel and identify relevant notification parties.

8.7.2. Incident response plans must be tested at least annually if not activated during that year.

8.7.3. Network and host activity must be monitored to identify policy violations, anomalous behavior, or unexpected application services.

8.7.4. Third Party must notify Ally of all cybersecurity events in accordance with the requirements of the master agreement.

8.7.5. Once the Third Party discovers or is notified of a security breach, it must investigate, fix, restore, and conduct a root cause analysis.

8.7.6. Third Party must provide Ally with results and frequent status updates upon investigations involving incidents related to an Ally information or asset.

8.7.7. If Ally is not satisfied with speed or effectiveness of an investigation, the Third Party must. make available an escalation process to address questions or concerns Ally may have during the investigation.

8.7.8. Third Party must ensure that its applications and infrastructure that are used to store, process, or transmit Non-Public Ally data use audit trails to record and retain information security relevant actions, including access attempts and privileged access.

8.7.9. Third Party must ensure that access controls are in place to preserve the integrity of audit trails and prevent unauthorized modifications to the audit logs.

8.7.10. Third Party must define retention periods for log data that complies with all applicable legal and regulatory requirements and maintain and comply with such retention requirements.

8.8 **Network Security**

8.8.1. Third Party must maintain an updated network diagram highlighting key internal network components, network boundary components, and demilitarized zone (DMZ) environment for all networks used to develop, process, store, or maintain Ally data.

8.8.2. Third Party must ensure that all information systems and applications that are used to store, process, and/or transmit Non-Public Ally Information, and are accessible via the Internet are only accessed via the Third Parties DMZ or similar dedicated secure network area.

8.8.3. The production network must be either firewalled or physically isolated from the development, test, and back-office environments.

8.8.4. All network services must pass through a security access layer allowing only the specific hosts, protocols and services required to provide the functionality. These access rules must be reviewed and updated by the Third Party at least every 6 months.

8.8.5. Third Party must have an intrusion detection system (IDS), intrusion prevention system (IPS), or equivalent network and host monitoring system in place to monitor, detect, and protect their network where Ally's non-public data is stored, processed, maintained, or transmitted.

8.8.6. Ally branded Internet applications and services hosted at Third Party sites must have a commercially available and up to date anti-DDoS solution.

8.8.7. Remote access to information systems used to store, process, or transmit Non-Public Ally Data must be protected from unauthorized use and utilize multi-factor authentication (MFA).

8.8.8. Wireless networks must be encrypted with current encryption algorithms. Use of weak, flawed, or insecure algorithms are not allowed.

8.8.9. Third Party must ensure all unused or unnecessary software, applications, and services are disabled on all IT systems that are used to process, store or access Ally Data.

8.8.10. Third Party must ensure that administrative functions are only accessed via secure methods (SSH or TLS) that encrypt traffic during transmission.

8.8.11. On workstations being used to access Non-Public Ally data, end users must not be permitted to have local administrative access.

8.8.12. Where local administrative access on workstations is required, Third Party must document, review, and approve local admin access for any workstations being used to develop, support or access Non-Public Ally information. Local Admin rights must be reviewed and reapproved at least every 6 months.

8.8.13. Workstation security settings (e.g., screen saver, antivirus) must be unalterable by end users

and must be configured to prevent ability to copy Non-Public Ally Data from workstations to removable media.

8.9 Vulnerability Management

8.9.1. Third Party with access to Non-Public Ally Data must perform penetration testing against internal and external networks and/or specific hosts on an annual basis. Environments containing Non-Public Ally Information must be covered as part of the scope of the tests.

8.9.2. Third Party must have, maintain, and follow a documented process to protect all IT systems from known security vulnerabilities by installing applicable vendor supplied security patches in a timely manner based on the risk.

8.9.3. Third Party must ensure all IT Systems are protected from malware, virus, trojan, and spyware using commercially available endpoint or network protection Data and have the most recent manufacture signatures, definitions files, and security updates installed.

8.9.4. Third Party must have a documented and followed vulnerability management process. This process must include:

- Infrastructure, network, and application security vulnerability assessments that are conducted at least quarterly. Environments containing and/or supporting access to Non-Public Ally Data must be covered as part of the scope of the assessments.
- Review and ranking of identified vulnerabilities, based on risk, using industry accepted risk rating (CVE/CVSS)
- Documented remediation timelines based on severity and application risk.

8.9.5. All Third Parties must provide Ally with evidence that supports completion of security vulnerability assessments and remediation on at least annual basis. Third Parties deemed to be critical must provide the evidence on quarterly basis. One or more of the following types of artifacts can be used to demonstrate the completion and remediation of identified vulnerabilities.

8.9.6. Reports with results that evidence completion of vulnerability assessments and timely remediation or executive summary reports without detailed results that evidence completion of vulnerability assessments and timely remediation (or)

8.9.7. Attestation from Third Parties senior leadership affirming completion of vulnerability assessments and timely remediation.

9.0 Privacy Standards

Ally requires that if a Third Party collects, uses, stores, and/or shares Ally Personal Information (i.e., PII, PHI, PCI), Third Party must comply with the following Privacy standards:

9.1 Have a documented Privacy policy that governs the collection, use and storage of personal, individual data across the enterprise, including third party vendors, in accordance with privacy laws and regulations. Third Party information controls must be audited according to a documented, repeatable, and sustainable audit program.

9.2 A consumer can provide or update their preferences (e.g., opt-outs) via phone, online, or mail.

9.3 When applicable, vendor will provide specific (e.g., CCPA) privacy notices or opt-outs as required by law.

9.4 Deliver annual Privacy training to workforce to include topics of social engineering (including "Phishing"), appropriate collection, usage, and storage of Ally Personal Information, including Confidential Information and Consumer Information.

9.5 Have documented data management procedures addressing the following:

- 9.5.1 Data usage, collection, and sharing (including Privacy Notice communications if Personal Information is subject to sharing)
- 9.5.2 Data storage, retention, and deletion/destruction
- 9.5.3 Handle consumer and employee data with care and only collect, use, or share what is necessary to perform a transaction.
- 9.5.4 Data classification
- 9.5.5 Data collection methods (paper and electronic)

9.6 Have documented escalation procedures for compromise of any Ally Personal Information (e.g., Privacy data breaches) outlining when to escalate to Ally and to whom specifically within the Ally organization.

9.7 Have documented identification and reporting procedures for compromise of Personal Information (e.g., Privacy Event) outlining what to report, when to report, and how to report.

- 9.7.1. Data breaches involving Personal Information must be escalated to Ally as soon as reasonably practicable, but in no event more than 24 hours from the time Third Party became aware of the Event.

9.8 Have a documented procedure for reviewing the following (including stakeholder communication):

- 9.8.1. Maintaining ongoing compliance with applicable Privacy laws and regulations.
- 9.8.2. Identification of potential compliance risks emerging from business and/or regulatory environment.

9.9 Have documented privacy risk assessment processes including a continuous monitoring routine to identify trends, escalate findings, and ensure compliance.

10.0 General and Regulatory Compliance

10.1 General Compliance Program

Ally requires Regulated Third Parties and Third Parties that perform Regulated Work on Ally's behalf to have a documented, sustainable, and repeatable compliance program.

10.1.1. **Regulatory Oversight**

10.1.1.1. Ally requires Regulated Third Parties and Third Parties that perform Regulated Work on Ally's behalf to have in place a formal management oversight team responsible for compliance with regulatory requirements.

10.1.1.2. Ally requires Regulated Third Parties and Third Parties that perform Regulated Work on Ally's behalf to conduct risk and controls self-assessments on an annual cadence at minimum.

10.1.2. **Change Management**

Ally requires Regulated Third Parties and Third Parties that perform Regulated Work on Ally's behalf to monitor and review all policies for regulatory compliance on a yearly cadence at minimum, and to track and communicate when changes to policies, procedures, etc. occur.

10.1.3. **Issue Management**

Ally requires Third Parties to identify, track, and treat issues that arise from a control failure.

10.1.4. **General Compliance Training**

Ally requires Third Parties to have a documented, sustainable, and repeatable, compliance-specific training policy to include role-based employee training that includes subject matter relevant to regulations in scope for the services provided or supported, complete with testing/attestation on a specified cadence.

10.2 Anti-Corruption

10.2.1. Ally requires that its Third Parties, Third Party employees, and Subcontractors always demonstrate integrity and comply with Anti-Corruption Laws.

10.2.2. Third Party must prohibit its entities, employees, Subcontractors and Third Party employees from any violation of any Anti-Corruption Law.

10.2.3. Anti-Corruption Laws prohibit payments through intermediaries (e.g., vendors, Third Parties, agents, consultants, sales representatives, resellers, or joint venture partners) involving bribery, corruption, fraud, dishonesty, or money laundering. If a payment directly to a person is prohibited, then a payment to any Subcontractor or Third Party employee with knowledge that the Subcontractor or Third Party employee will pass it on to that person is also prohibited. "Knowledge" includes not only actual knowledge, but also conscious disregard or willful ignorance of the facts and circumstances.

10.2.4. Any Third Party transaction or activity that violates or may reasonably be expected to result in noncompliance with these Requirements, or any applicable Anti-Corruption Laws, must be promptly reported to Ally's Legal Staff, Ally's Anti-Money Laundering senior leadership, and Third Party's senior leadership. To the extent any such transaction or activity involving Ally or Ally Data is found to have violated any Anti-Corruption Laws or could potentially have a material impact on Ally or Ally assets, Third Party must escalate such transaction or activity to Ally via the Ally Ethics Hotline at 800-971-6037.

10.2.5. Ally requires Third Parties to have a documented, repeatable, and sustainable Anti-Corruption/Anti-Bribery program in place to ensure the appropriate policies, procedures, agreements, training, and oversight are in place to mitigate the risk of Anti-Corruption/Anti-Bribery and Facilitation of Payments compliance violations.

10.3 Anti-Money Laundering (AML) / Bank Secrecy Act (BSA)

10.3.1. If Third Party is conducting services for Ally related to AML transaction monitoring or investigations, Enhanced Due Diligence (EDD), or other staff augmentation services to assist with Financial Crimes Compliance (FCC), Third Party must follow Ally's relevant Polices and Standards as well as have appropriate training and controls in place to prevent non-compliance.

10.3.2. If Third Party is conducting any portion of the CIP/CDD process during account opening on behalf of Ally, such as collection and/or verification of customer's information; Third Party must follow Ally's relevant Polices and Standards to be in compliance with CIP and/or CDD, as well as have appropriate training, procedures, and controls in place to prevent non-compliance.

10.4 Office of Foreign Asset Control (OFAC)

10.4.1. Generally, Third Parties conducting account opening or transactional services for Ally will ensure they either follow Ally's policies and standards or its own policies and controls to ensure compliance with OFAC sanctions regulations.

10.5 Fair and Responsible Banking

10.5.1. **Unfair, Deceptive or Abusive Acts or Practices (UDAAP), Fair Credit Reporting Act (FCRA), and Fair Debt Collection Practices Act (FDCPA)**

10.5.1.1. Ally requires Third Parties that interact with Ally customers (e.g., sales, marketing, credit applications, call center, collections, and repossessions) to have documented Unfair or Deceptive Acts or Practices (UDAAP) policy which is reviewed and approved annually and includes a UDAAP definition that is consistent with Ally's Enterprise UDAAP Policy definition.

10.5.1.2. Ally requires Third Parties that interact with Ally customers (e.g., sales, marketing, credit applications, call center, collections, and repossessions) to have documented Unfair or Deceptive Acts or Practices (UDAAP) training which is required to be completed annually by all customer-facing employees, subcontractors, or agents and maintain proof of completion of the training.

10.5.1.3. If the Third Party is collecting or processing any credit transaction on behalf of Ally, the Third Party must also have a documented FCRA and FDCPA policy that is reviewed annually.

10.5.1.4. If the Third Party is collecting or processing any credit transaction on behalf of Ally, the Third Party must provide annual training on FCRA and FDCPA and maintain proof of completion of the training.

10.5.2. **Consumer Complaints**

10.5.2.1. Ally requires Third Parties that interact with Ally customers to have a documented risk-based, repeatable, and sustainable complaints management process, that is reviewed at least annually, to handle consumer complaints received with respect to Ally services. The policy must contain, at a minimum, the following elements:

- the definition of a complaint (consistent with Ally's definition),
- a process for responding to high risk complaints (e.g., UDAAP, SCRA, complaints of discrimination, complaints received from regulatory agencies),
- a required timeframe for responding to complaints, and
- a method for identifying and/or tracking trends and identifying root causes of complaints.

10.5.2.2. Ally requires Third Parties that interact with Ally customers to provide training that provides instruction on how to handle, track and report complaints. This complaint training must be completed annually.

10.6 Fair Lending

10.6.1. Ally requires Third Parties that provide any service related to any aspect of the credit lifecycle (e.g., sales, marketing, credit applications, call center, collections, repossessions) to have a documented Fair Lending policy that is reviewed and approved annually. The policy must include the prohibited basis set forth in Fair Lending laws (Fair Housing Act and ECOA/Regulation B).

10.6.2. Ally requires Third Parties that provide any services related to any aspect of the credit lifecycle (e.g., sales, marketing, credit applications, call center, collections, repossessions) to have documented Fair Lending training that is administered annually and maintain evidence of completion.

10.7 Licensing Oversight

10.7.1. Ally requires Third Parties that provide services on Ally's behalf that are required by applicable law to acquire and maintain licensure (e.g., investment, real estate, mortgage broker or servicing agent, repossession, NOT business license), to have a documented, sustainable, and repeatable licensing compliance program or procedure to ensure required licenses are obtained before engaging in services with Ally and maintained while providing services for Ally.

10.8 PCI Compliance

10.8.1. If Third Party has access to or stores full 16-digit PAN or processes payments using credit or debit cards on behalf of Ally, Ally requires Third Party to provide a current Attestation of Compliance (AOC).

10.8.2. Ally requires Third Party to maintain a Data Flow Diagram.

10.9 Financial Transaction

10.9.1. Ally requires financial transaction records be stored for at least 5 years.

11.0 Enterprise Resilience Standards

Enterprise Resilience addresses the risk of direct losses resulting from business disruptions caused by natural disasters, internal or external technology outages, intentional or unintentional acts of people, failed processes, or systems, or from other external events.

11.1

11.1.1. Third Party must establish an ongoing process to identify the impact of business disruptions, maintain viable recovery strategies and recovery plans, and optimize the continuity of Services. Pursuant to Third Party's enterprise resilience obligations in the Agreement, the following standards provide direction for the development and implementation of business continuity and crisis management plans to mitigate the impact to Ally of a Third Party business disruption in the event under the Agreement one was to occur.

11.1.2. These Enterprise Resilience Standards are specifically designed to align with Federal Reserve Board (FRB) and Federal Financial Institutions Examination Council (FFIEC) guidance.

11.2 Enterprise Resilience Framework

To maintain effective enterprise resilience, and while performing Services to Ally, Third Party must implement the following Business Continuity and Crisis Management Planning framework:

- Business Impact Analysis (BIA)
- BCP Site Risk Assessment
- Business Resumption Planning (BRP)
- IT Disaster Recovery Planning (IT DRP)
- Crisis Management Plan (CMP)/Incident Response Plan (IRP)
- Plan Exercising/Testing
- Subcontractor Management

11.3 Business Impact Analysis (BIA)

The BIA is the process of identifying the potential impact of business disruption to Ally's functions and processes. The BIA uses a consistent methodology to measure potential quantitative (e.g., financial revenue loss, incurred expenses) and qualitative (e.g., operational, legal/regulatory) impacts to Ally resulting from a business disruption, including consideration of escalating impacts over time. BIAs must be reviewed and updated annually, or other otherwise stated in the Agreement/MSA, to ensure Third Party has current data to support risk-based business continuity planning and the alignment of recovery strategies.

11.4 BCP Site Risk Assessment

The BCP Site Risk Assessment determines the likelihood and impact of threats and hazards based upon practical experiences, potential circumstances that could disrupt work areas, business processes, facilities, or geographic locations. Results BCP Site Risk Assessments are used to determine adequacy of response capabilities and prioritize scenarios for BCP exercises. BCP Site Risk Assessments must be periodically reviewed and updated.

11.5 Business Resumption Planning (BRP)

BRPs, in conjunction with IT DRPs and CMPs/IRPs, document the activities and information required to recover operations in the event of a disaster or crisis situation. BRPs must be reviewed and updated at least annually to ensure that plans are current and viable in the event of a business interruption.

11.6 Information Technology Disaster Recovery Planning (IT DRP)

IT DRPs document the activities and information required to restore IT applications (including IT

utilities and tools) and infrastructure to pre-determined and agreed-to levels of IT services following a business disruption. IT DRPs must be reviewed and updated at least annually by IT staff to ensure they are aligned with the business priorities and activities as identified in the BIA results and BRPs, and recovery time objectives (RTOs) and recovery point objectives (RPOs) are in alignment with the Agreement/MSA.

11.6.1. **Plan Exercising and Testing**

The effectiveness of BCP is validated through exercising/testing BRPs, IT DRPs, evaluating results, and developing enhanced processes or other improvements based on exercise/test results. BCP exercises/tests must be designed so that plan components are rehearsed in whole or in part, to verify that the plan(s) contain(s) the appropriate information and produces the desired results when put into effect. Further, plans should be exercised/tested in a coordinated manner, as applicable, to confirm that the documented recovery strategies are viable, and recovery time objectives and recovery point objectives are met. Testing and certification of Third Party's BRPs, DRPs, must occur at least once every calendar year during the Term, unless otherwise stated in the Agreement/MSA.

Upon request, Third Parties must provide evidence of exercises/testing to Ally for confirmation of alignment with these Requirements. Acceptable test evidence may include post-exercise reports, independent third-party assessments, SOC1, or SOC2).

11.6.2. **Subcontractor Management**

Include subcontractors in Business Continuity Planning, as well as plan exercise/testing routines, when appropriate, to evaluate Subcontractor(s) compliance with their obligations under the Agreement including these Requirements.

11.7 **Crisis Management and Incident Response Standards**

Third parties should have a crisis management and incident response program beyond business continuity planning. The program must consist of the following elements:

11.7.1. **Risk Assessment and Controls**

Third Parties are expected to perform risk assessments that identify risk exposure, determine threats and their potential impact, and identify controls and mitigation measures put in place to address risk. If this is performed satisfactorily as part of the Section 11.3. Business Impact Analysis/Assessment (BIA) and Section 11.4. BCP Site Risk Assessment, this requirement is considered met. If not, evidence of the performance of Risk Assessments should be provided or should be described in the plans described in Section 11.7.3 below.

11.7.2. **Response Plans**

Third parties must have a company-wide Crisis Management Plan or Incident Response Plan(s) to identify roles and responsibilities for a response team, the process in which the team will operate to manage an incident or crisis, and how the team will communicate and coordinate with Ally during an incident or crisis. In addition to a company-wide plan, Third Parties should have specific plans or procedures to address:

- Technology and/or cyber incidents and attacks.
- Pandemic response

11.7.3. **Plan Exercising & Testing**

The effectiveness of Crisis Management programs is validated through an ongoing schedule of exercising/testing of CMPs/IRPs, evaluating and summarizing results in an after-action report, and developing enhanced processes or other improvements based on exercise/test results. These exercises/tests could include various formats, such as drills, tabletop exercises, functional exercises, or full-scale exercises, and must be designed so that plan components are rehearsed in whole or in part, to verify that the plan(s) contain(s) the appropriate information and produces the desired results when put into effect. Further,

plans should be exercised/tested in a coordinated manner, as applicable, to confirm that the documented response operations are effective, and the recovery strategy is viable and executable. Testing and certification of Third Party's CM plans must occur at least once every calendar year during the Term.

12.0 Physical Security Standards

Third Party must adhere to the following physical security standards at all Third Party facilities where Confidential Information and Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term.

12.1 Documentation of the Physical Security Program

Third Party must document its physical security program to ensure that is it repeatable, sustainable, and incorporates a risk-based approach that meets or exceeds Ally's Third Party Requirements outlined in this section.

12.2 Physical Access Control Program

When and where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term, Ally requires Third Parties to operate and maintain a physical access control program that strictly limits access into the facility to only personnel (current employees, contractors, Visitors, and on-site vendors) who have been properly authorized, documented, and escorted as required.

12.2.1. Piggybacking / Tailgating Control

If physical electronic access control systems are in use, each person who enters a restricted area must utilize the access control method in place. E.g., Each person entering a restricted area equipped with a badge reader is required to swipe their own badge before entering. At no time should a Third Party employee allow anyone to enter a restricted area by following an authorized person.

Exceptions to this are: in case of an emergency where life safety is the primary concern, or when an authorized Visitor without active access badge is being escorted by a Third Party.

12.2.2. Identification of Third Parties and Visitors

The following must be implemented and enforced by the Third Party in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term.

12.2.2.1. All Visitors are to remain in the entry lobby or reception area until the host arrives to escort the Visitor.

12.2.2.2. All Visitors must present a valid government issued photo ID when signing in.

12.2.2.3. All Visitors must sign in and out on a Visitor log providing name, company represented, date, in and out time, and person being visited.

12.2.2.4. Third Party receiving the Visitor is responsible for ensuring the Visitor is escorted at all times while at facility.

12.2.2.5. Visitor logs must be maintained for audit and review for no less than 90 days.

12.2.2.6. Physical access for Visitors must be limited to one access point.

12.2.2.7. Third Party and authorized Visitors must be prohibited from admitting unauthorized Visitors through any other access point or without following Visitor access control procedures.

12.2.2.8. If Visitors are registered in the physical electronic access control system, then Visitors are required to use the access method each time they enter a restricted area.

12.2.3. Physical Electronic Access Control Systems Controls

12.2.3.1. When a physical electronic access control system is utilized, each Third Party is required to use the access method each time they enter a restricted area.

12.2.3.2. When a physical electronic access control system is utilized, physical access control logs must be maintained for audit and review for no less than 90 days.

12.2.3.3. When a physical electronic access control system is utilized, each Third Party must be registered in a physical electronic access control system and have a working and

trackable means of physical access on their first day of employment.

12.2.3.4. When a physical electronic access control system is utilized, access audits shall be performed at least twice per year to ensure those individuals who have access are authorized.

12.2.3.5. When electronic physical access systems are not utilized, a documented compensating control accompanied by a documented procedure is required.

12.2.3.6. Third Parties who terminate employment or have employment terminated must have their access removed immediately.

12.2.4. **Physical Intrusion Alarm Controls**

12.2.4.1. Physical access control system alarms must be acknowledged within a timely manner and must have a written process to report all physical access control violations.

12.2.4.2. There must be a process for investigation and response (if appropriate) for all alarms.

12.2.4.3. The alarm/alerting system must notify responsible and responding forces when and where an immediate response is required (e.g., duress alarms, intrusion alarms, door open over-ride notices).

12.2.4.4. The physical alarm/alerting system(s) must provide an audit trail which documents alarm alert notifications, responses, and resolutions for no less than 90 days.

12.2.4.5. Physical intrusion and duress alarms shall be tested once per month to ensure functionality. Documentation of testing must be recorded and retained for review for no less than 90 days.

12.2.4.6. Third Parties must never allow another individual to use their credentials, PIN codes, pass cards or any identifier that allows for arming/disarming of any intrusion alarm for any reason.

12.2.4.7. Access credentials must be managed appropriately, including disabling PINs and pass cards upon the agent's separation.

12.2.5. **Access Card and Physical Key Controls**

12.2.5.1. A record of the access card number and the name of the holder must be maintained for all physical access cards issued, to include accounting for each time an access card is issued or returned. At any given time, the log must accurately reflect the location of all access cards.

12.2.5.2. Proper secure storage (e.g., a locked metal file drawer or other controlled container) must be maintained for all physical access cards or keys, spare access cards or keys, and access card or key equipment.

12.2.5.3. An audit of physical access cards and/or keys must be performed and documented no less than semi-annually.

12.2.5.4. If at any time a key control system is compromised, (e.g., a lost key), Third Party must evaluate the circumstances and consider engaging a locksmith to re-key the facility or affected lock.

12.2.6. **High-Security Area Controls**

12.2.6.1. A physical electronic access control system must be used to secure and track entrances to High-Security Areas (HSA).

12.2.6.2. A monthly audit of authorized individuals must be conducted for all HSAs.

12.2.6.3. Those who no longer have the need for regular access to HSAs should have their access removed immediately.

12.2.6.4. Results of the audit must be maintained for no less than 90 days and no more than 1 year.

12.2.6.5. Employees, contractors, vendors, and Visitors to HSAs must be pre-approved by the HSA space owner, shall be escorted at all times by an authorized employee, and will follow the Ally HSA visitor access request process.

12.2.6.6. Visitor logs for High-Security Areas must be accessible and available upon request for no less than 90 days and no more than 1 year.

12.2.6.7. Any Facility with an electronic PACS (Physical Access Control Systems) must include

card readers to HSA and separate clearance code.

12.2.6.8. HSAs must be maintained free of all clutter and debris. Items not directly related to the operation or maintenance of the data center must not be stored within.

12.2.6.9. Utilize dual factor authentication for entry.

12.2.6.10. Have video surveillance of all entry/exit points.

12.2.6.11. All Visitors to a High-Security Area must have a pre-approved purpose for entering the area, must be escorted by an authorized Third Party at all times, and must sign the local Visitors log to include date; name; company; purpose for entry; escort's name; and time in and out.

12.2.6.12. Personal bags, boxes, and coats must not be allowed in cashier's cages, check production rooms, or check storage areas.

12.2.6.13. Vaults and safes must meet burglar- and fire-resistant standards based on sensitivity of the asset(s) being protected.

12.2.7. **Video Surveillance (CCTV) Controls**

12.2.7.1. Operate and maintain a video recording system as appropriate that retains at least 30 days of video recordings; (90 days where Payment Card Industry (PCI) Standards are required).

12.2.7.2. Cameras must be positioned (when possible) to collect images that can be used to identify the individual(s) attempting to, or gaining, access to areas secured by electronic physical access systems.

12.2.7.3. The placement of video surveillance at a facility adheres to clear, documented security objectives (e.g., command, control, response, or investigative).

12.2.7.4. All video surveillance systems must be recorded using digital technology that can be remotely monitored.

12.2.7.5. Each facility equipped with video surveillance technology is responsible for confirming that all cameras are functional by testing (i.e., viewing live images) at least once per week. Documentation of testing must be recorded for audit.

12.2.7.6. All video surveillance cameras must be overt and visible. Hidden cameras are considered a violation of workplace privacy law in almost all circumstances. Third Party should disclose all security cameras to employees.

12.2.8. **Reliability of Physical Security Infrastructure**

12.2.8.1. Third Party must regularly review that any associated equipment (either installed and maintained by Third Party, Subcontractor, or by any other third-party such as a landlord or third-party data center) is properly functioning and in good working order.

12.2.8.2. All applicable electronic physical security controls must be connected to an uninterruptable power supply.

12.2.9. **Photographic and Recording Equipment Standards**

12.2.9.1. Third Party must prohibit the use of photographic and recording equipment for the purpose of taking pictures and recording conversations where Ally Data, Confidential Information or Consumer Information is involved. Photographic and recording equipment includes but is not limited to the following: cameras (digital or film), video cameras (digital or film), PDAs, flash drives, portable hard drives, removable media (CD, DVD, floppy disks, tapes), digital or analog voice recorders, personal computer equipment, tablets, and mobile phones.

12.2.10. **Security Personnel Management**

12.2.10.1. Standard operating procedures or post orders must be developed for any facilities(s) with a contract or proprietary security force.

12.2.10.2. Daily activity reports and incident reports must be a part of the post orders.

12.2.10.3. Reports must be maintained for a minimum of two years.

13.0 Subcontractor Management

As a regulated financial institution, Ally is expected to identify and understand the services of any Third Party Subcontractor. In addition, Ally requires that Third Parties have a risk based Third Party Risk Management Program in place to oversee its Subcontractors in a similar manner to which Ally oversees its Third Parties. Ally requirements align to the Federal Reserve Board's (FRB) *Interagency Guidance on Third-Party Relationships: Risk Management* (SR 23-4).

13.1 Ally Third Parties will be expected to have a Third Party Risk Management program that includes but is not limited to:

- 13.1.1. Methodology for assessing the risk of its Third Parties including any Subcontractors.
- 13.1.2. Risk based Due Diligence activities prior to onboarding, including review of applicable Third Party controls.
- 13.1.3. Written Third Party contracts that contain similar contract provisions and considerations to those contained under Third Party's contract with Ally.
- 13.1.4. Risk based Ongoing Monitoring activities after onboarding that address:
- 13.1.5. Recurring controls reviews as applicable.
- 13.1.6. SOC reviews where available and applicable.
- 13.1.7. Financial monitoring.
- 13.1.8. SLA/Performance monitoring.
- 13.1.9. Termination activities governing the offboarding of Third Parties.