Table of Contents

1.0 Purpose

The purpose of these Third Party Requirements ("Requirements") is to identify the minimum expectations Ally and its Affiliates hold Supplier and Subcontractors accountable to adhere to while performing Services in accordance with the Agreement.

2.0 Scope

These Requirements apply to all Ally Suppliers, 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 Supplier Requirements

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

4.0 Definitions

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

"Ally Data" means all data and information that Ally or any Affiliate of Ally or any Ally Third Party Service Provider provides to Supplier or that otherwise comes into Supplier's or a Supplier agent's possession pursuant to this Agreement. Ally Data includes Consumer Information and Confidential Information of Ally and Affiliates of Ally and Ally Third Party Service Providers.

"Ally Systems" means the information systems, for example hardware, software, networks, data, tool kits, or other information system resources, owned or licensed by or on behalf of Ally or an Ally Affiliate or an Ally Third Party Service Provider, that may be used or accessed by Supplier or is

integrated with Supplier IT Systems in connection with the Services, in each case, excluding Supplier IT Systems.

"Computing Asset" means 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.

"Electronic Physical Access Control System" means a method of securing entrances and exits to sensitive areas of Supplier'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(s)" means a specific area within a Supplier 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 this area (e.g., data centers, vaults, UPS rooms, etc.).

"IT System" means any collection of computing and/or communications components and other resources that support one or more of Supplier'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" is any and 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: Any and 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: Any and 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: Any and 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.

Personally Identifiable Information (PII) refers to 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.

Protected Health Information (PHI) is 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 Suppliers" means that the Supplier receives oversight and direction from government entities with regard to the service(s) provided to Ally.

"Regulated Work" means that Ally receives oversight and direction from government entities regarding the service(s) the Supplier is providing on Ally's behalf.

"Subcontractor" means a person or entity, other than Ally and the entity named as "Supplier" 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.

"Supplier" means Supplier, Supplier Affiliates, and their consultants, Subcontractors, agents and representatives that perform Services under this Agreement.

"Visitor" means Individuals visiting Supplier's site who are not employees or contractors performing work on a regular basis for Supplier. 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, Suppliers are expected to adhere to guidelines for effective management and monitoring of potential unethical behavior, including fraud, bribery, corruption, dishonest, and money laundering.

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

5.2. Ally requires Suppliers 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 Suppliers to maintain records evidencing the review and attestation of the personal responsibility message defining and prohibiting unethical behavior by all employees and Subcontractors.

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

5.4. Ally requires Suppliers to communicate clear expectations for reporting instances of unethical behavior to Supplier employees and Subcontractors.

5.5. Ally requires Suppliers to provide Supplier employees and Subcontractors with an anonymous method for reporting unethical behavior.

5.6. Ally requires Suppliers to document their whistleblower protections protecting individuals who, in good faith, report instances of unethical behavior.

5.7. Supplier must report to Ally, within 24 hours, any illegal, unethical, or improper behavior or incidents they observe or which they become aware of that pertains to Ally.

Supplier 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

5.8. Ally requires Suppliers to have a documented and communicated method for detecting and managing any situations in which an employee 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	Supplier Type E
Employment History		Invest: 10 Years	Invest: 10 Years	Invest: 10 Years	
Foreign Employment		Invest: 10 Years	Invest: 10 Years	Invest: 10 Years	
Criminal Background	Min. 10 Year	Min. 7 Year (Invest: Min. 10 Yr.)	Min. 7 Year	Min. 7 Year	
Credit Check	✓	✓			
Education Verification		Invest Only	Invest Only	Invest Only	
Motor Vehicle Record			✓		
Sex Offender	✓	✓	✓	✓	
OFAC/Global Sanctions	✓	✓			
SSN Tracing	✓	✓	✓	✓	

Supplier Type A: Suppliers 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. Suppliers are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.9).

Supplier Type B: Suppliers 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 aug. 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 6.9).

Supplier Type C: Suppliers operating motor vehicles in the delivery of services to Ally. Suppliers are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.9).

Supplier Type D: All other Suppliers receiving Non-Public Ally Data. Suppliers are subject to the applicable sections of the Ally Background Check Adjudication Criteria (see section 6.9).

Supplier Type E: All other Suppliers not receiving Ally Data. – No requirements.

6.1. **Requirements**

6.1.1. Supplier will conduct background checks as set forth in Ally's "Domestic Background Check Adjudication Criteria" (section 6.9) 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 Supplier will conduct background checks consistent with these Requirements for the purpose of:

6.1.1.1. Verifying the accuracy of information provided by Supplier employees or Subcontractors and their employment eligibility prior to hire; and

6.1.1.2. Maintaining consistent and sustainable eligibility requirements during a Supplier employee's or Subcontractor's course of employment; and

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

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

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

6.2. **Employment Background Check Finding** (for Supplier employees or Subcontractors performing Services for Ally Invest)

6.2.1. Supplier must verify 10 years minimum of employment history for Supplier employees, including dates, job title(s), and make an attempt to obtain the reason for discharge at former organizations.

6.3. **Foreign Employment** (for Supplier employees or Subcontractors performing Services for Ally Invest)

6.3.1. Supplier must verify 10 years minimum of employment history for Supplier employees, including dates, job title(s), and make an attempt to obtain the reason for discharge at former organizations.

6.4. **Criminal Background Check Finding**

6.4.1. Supplier must verify prior to Services commencing that Supplier employees and Subcontractors have been screened for criminal records as set forth in Ally's "Domestic Background Check Adjudication Criteria" (section 6.9) based on application of the Background Check Requirements Table in section 6.0.

6.4.2. 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".

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

6.5. **Credit Background Check Finding** (if applicable based on Supplier Type)

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

6.5.2. Supplier must verify that Supplier 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.

6.5.3. Mortgage roles only – Prior to Supplier employees or Subcontractors taking Ally Mortgage roles, Ally requires that Supplier validates that Supplier 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

6.5.4. Ally Invest only – Prior to Supplier employees or Subcontractors taking Ally Invest roles, Ally

requires that Supplier validates that Supplier employees' and Subcontractors' credit reports have no items in Collections, liens, judgments, accounts charged to profit/loss, repossessions and outstanding bankruptcies or past due amounts that in the aggregate totals more than $15,000.00. ANY satisfied or unsatisfied liens, judgements, compromises, or bankruptcy, regardless of the amount are reportable on Form U4.

6.6. **Education Background Check Finding** (for Supplier employees or Subcontractors performing Services for Ally Invest)

6.6.1. For Supplier employees and Subcontractors providing Services to Ally, Supplier must verify education set forth in Ally's Domestic Background Check Adjudication Criteria.

6.6.2. Verify the highest degree claimed; if no degree is claimed, then Supplier must verify a High School diploma. If high school diploma is over 10 years old and unable to be verified, mark as a Pass. The degree earned needs to be verified; the date the degree was received does not need to be obtained in order to pass.

6.6.3. Confirm that the name on the degree matches.

6.6.4. Screen foreign education using the same verification process. Evidence of the diploma and mark statement/transcript must be obtained.

6.7. **Motor Vehicle Record Background Check Finding** (if applicable based on Supplier Type)

6.7.1. As set forth in Ally's Domestic Background Check Adjudication Criteria, Supplier must validate that the Supplier 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.

6.8. **Additional Checks set forth in Ally's Domestic Background Check Adjudication Criteria** (if applicable based on Supplier Type):

6.8.1. **Sexual Offender Registry** – Supplier must search Sexual 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 database searches. Consider reportable sex conviction(s).

6.8.2. **Global Sanctions** – including OFAC hits, General Services Administration (GSA) hits and FDIC enforcement actions. Supplier validates no hits.

6.8.3. **SSN Tracing** – Supplier validates SSN matches Supplier employee or Subcontractor.

6.9. **Ally Domestic Background Check Adjudication Criteria**

Applicable to: Supplier Types A, B, C, and D

Purpose: To define requirements of Ally Financial for specific types of background checks to be performed by Supplier 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, Supplier will conduct background checks consistent with the requirements identified within the Ally Third Party Requirements. The Supplier 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 education, employment or credit component(s) are eligible for re-hire after a 6-month waiting period from the date the Adverse Letter is sent. <u>Canadian Residents (The nonimmigrant NAFTA Professional (TN) visa)</u> • 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 supplier candidate(s) reside in these states / localities and the supplier is unable to access criminal reporting for a

candidate(s) due to a state / local reporting limitation, Ally will deem the supplier to have satisfied the criminal history search so long as the supplier 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**. **Mortgage Roles only** - 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 **$10,000.00**. **Ally Invest only** - If credit report has no items in collections, liens, judgments, and accounts charged to profit/loss, repossessions and outstanding bankruptcies or past due amounts, that in the aggregate total more than **$15,000.00**. ANY satisfied or unsatisfied liens, judgements, compromises, or bankruptcy, regardless of the amount are reportable on Form U4.	Pass
Unpaid tax lien, civil judgment, loan default, collection account, charge off account, negative judgment, or past due balance of more than 90 days delinquent, that in the aggregate total **$50,000.00** or more including any record of bankruptcy, foreclosures, and auto repossession. **Mortgage Roles only** - Unpaid tax lien, civil judgment, loan default, collection account, charge off account, negative judgment, past due balance of more than 90 days delinquent, that in the aggregate total **$10,000.00** or more including any record of bankruptcy, foreclosures, and auto repossession. **Ally Invest only** - Unpaid tax lien, civil judgment, loan default, collection account, charge off account, negative judgment, or past due balance of more than 90 days delinquent, that in the aggregate total **$15,000.00** or more including any record of Bankruptcy, foreclosures, and auto repossession. ANY satisfied or unsatisfied liens, judgements, compromises, or bankruptcy, regardless of the amount are reportable on Form U4. **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

EDUCATION BACKGROUND CHECK FINDING (EDUCATION COMPONENTS APPLY TO ALLY INVEST RESOURCES ONLY) Supplier will check highest degree claimed; if no degree claimed, verify high school diploma. If high school diploma is over 10 years old and unable to be verified, mark as Pass. Degree earned needs to be verified, the date the degree was received does not need to be obtained in order to pass.	**DISPOSITION**
Degree match.	Pass
No degree awarded as claimed by applicant.	Review
Difference in degree as claimed by applicant.	Review
Degree or Diploma Mills	Fail

Note: Degree or diploma mill is an entity that charges a fee for a degree, diploma or certificate which represents completion of a program and there is little or no education or coursework requirement to obtain such degree, diploma or certificate OR entity lacks accreditation by a recognized accrediting agency (per Dept of Higher Education).	
If degree and/or diploma are in verification status and not yet confirmed.	Pending
FOREIGN EDUCATION (EDUCATION COMPONENTS APPLY TO ALLY INVEST RESOURCES ONLY) Supplier requires diploma and the mark statement/transcript to proceed.	**DISPOSITION**
Diploma and mark statement are not received within 3 business days of the request. Request should be made within 48 hours of finding.	Review
Degree match.	Pass
No degree awarded as claimed by applicant.	Review
Difference in degree as claimed by applicant.	Review
If degree and/or diploma are in verification status and not confirmed yet	Pending
EMPLOYMENT BACKGROUND CHECK FINDING (EMPLOYMENT COMPONENTS APPLY TO ALLY INVEST RESOURCES ONLY) For Ally Invest resources, 10 years of employment history must be verified. If the employer is unable to verify dates of employment based on document retention practices and the employee is unable to provide a W-2 and/or paystub, mark as Pass.	**DISPOSITION**
No employment information identified for verification.	Pending
Employment confirmed.	Pass
Employer found no record of applicant, or business could not be verified as ever having existed or business was not in existence at the time the applicant indicated they worked there.	Review
Employer is no longer in business and exact employment dates could not be verified. However, existence of business at the time of indicated employment confirmed.	Review
Discharge for Cause for: violence, theft, dishonesty, misconduct, breach of trust, illegal drug activity (except marijuana possession offenses not governed by the FDIC), harassment, or insubordination. Discharge for Cause; other than reasons above.	Fail Review
Difference in job title reflecting a discrepancy in job level and responsibilities.	Review
Dates discrepant by one year (12 months) or more. One year or less discrepancy is a Pass. **Note:** Perform resume comparison for possible error or typo. Supplier Adjudicator may assess if there is an attempt to cover gaps of unemployment.	Review
Current employer identified as “Do Not Contact” or N/A. Ally’s criteria require current employer to be verified. May accept appropriate information i.e., W-2 and current pay stub for period employed by current employer.	Review
If employment in verification status and not confirmed yet.	Pending
FOREIGN EMPLOYMENT (EMPLOYMENT COMPONENTS APPLY TO ALLY INVEST RESOURCES ONLY)	**DISPOSITION**
Employment Confirmed.	Pass
Employer found no record of applicant, or business could not be verified as ever having existed or business was not in existence at the time the applicant indicated they worked there.	Fail
Employer is no longer in business and exact employment dates could not be verified. However, existence of business at the time of indicated employment confirmed.	Review
Discharge for Cause for: violence, theft, dishonesty, misconduct, illegal drug activity (except marijuana possession offenses not governed by the FDIC), harassment, or insubordination. Discharge for Cause; other than reasons above.	Fail Review
Difference in job title reflecting a discrepancy in job level and responsibilities	Review
Dates discrepant by one year (12 months) or more.	Review

Current employer identified as “Do Not Contact” or N/A. Ally’s criteria require current employer to be verified, Supplier will work with applicant to obtain appropriate documentation**,** i.e., W-2 and current pay stub for period employed by current employer.	Review
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**
Sexual Offender Registry - Search matches registered offender (Potential risk should be assessed). **Note:** Decisions must not be based solely on records in the state 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
Education (Ally Invest resources only)	6 months	Must review full background
Employment (Ally Invest resources only)	6 months	Must review full background
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**

7.1. Supplier will comply with all applicable laws and regulations related to fair employment. Ally expects Suppliers performing Services for Ally to value the wide range of backgrounds of Supplier'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 Supplier's and Subcontractors' core values and contribute to a healthy and engaging culture. All Suppliers are responsible for creating and maintaining a productive work environment where the dignity of all individuals is respected. Suppliers should also treat customers, vendors, and guests, as well as the public in general fairly and with respect. Supplier shall not tolerate unlawful discrimination of any kind in any of its employment or business practices.

7.2. **Employment Standards**

7.2.1. Supplier 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 Suppliers at all locations where Ally business is conducted and other non-company locations if the conduct affects the work relationship.

7.2.1.1. 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.

7.2.1.2. 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.

7.3. **Accountability and Monitoring**

7.3.1. If, while performing Services under the Agreement, a Supplier 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

Supplier supervisor or department. The Ally Ethics Hotline may also be accessed if the behavior involves Ally or an Ally employee.

7.3.2. It is the responsibility of every Supplier 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. Supplier 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 Supplier's employee witnesses any violations or potential violations to these requirements involving Ally or on Ally premises, Supplier should report such violation or potential violation to the Ally Ethics Hotline.

8.0. **Information Security Standards**

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

8.1. **General Information Security Requirements**

8.1.1. Supplier'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. Supplier must ensure an information security awareness campaign is provided to all personnel who access Ally Data or Ally Systems. Supplier must educate personnel of their responsibilities to secure Ally Data and Ally Systems.

8.1.2. Supplier must document, implement, and follow rules of acceptable use of Computing Assets and must require that Supplier's Computing Assets are to be used in a professional, lawful, and ethical manner, and not to be used for activities which have been identified as unacceptable conduct.

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

8.1.4. Supplier must periodically assess risks within its information technology (IT) environment that is used to access Ally Data or Ally Systems.

8.1.5. Supplier must have a managed and up to date inventory of Supplier's Computing Assets that are used to access or support Ally Data or assets, including cloud services and functions.

8.1.6. Supplier must ensure that their Subcontractors are compliant with this Section 8 (Information Security Standards) of these Requirements. If requested by Ally, Supplier must provide adequate validation that any of its subcontractors are compliant with this Section 8 (Information Security Standards) of these Requirements.

8.1.7. Suppliers who connect to or use Ally Systems (including servers, workstations, infrastructure, internet gateway, or network) must abide by all applicable Ally terms of use and any supporting standards and procedures.

8.1.8. Supplier 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 and/or National Institute of Standards and Technology ("NIST") Special Security Publications.

8.2. **Application and Software Development and Management**

8.2.1. Supplier must have, maintain, and follow 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. Supplier must have, maintain, and follow documented change management procedures. Additionally, Suppliers 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 security of the Services, or cause the Services to be unavailable.

8.2.4. Supplier must ensure and confirm to Ally that any changes to IT Systems involved in providing Services to Ally are tested prior to deployment, communicated, 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. Additionally, Supplier 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. Supplier must have a defined backup policy and associated procedures for performing backup of Ally Data in a scheduled and timely manner.

8.3.2. Supplier 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 Non-Public 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 Supplier managed laptops that are used to store, access, support, or transmit Non-Public Ally Data must be protected with a full disk encryption solution.

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

8.4.4. If applicable to the Services provided to Ally, Supplier must secure all Payment Card Industry 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.

8.4.5. Data destruction processes must securely wipe all data on all media using a method that will not allow data to be retrieved. For all IT Systems that access Non-Public Ally Data, Ally requires the destruction be performed in accordance with the National Institute of Standards and Technology Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.

8.4.6. Where available, hardware, physical software and data destruction must follow a process that will not allow data to be recovered and proof or certificate of destruction must be provided to Ally. These processes must adhere to either National Association for Information Destruction guidelines or NIST Special Publication 800-88 Rev. 1. At a minimum, the disposal requirements must meet or exceed the requirements mandated by the National Association for Information Destruction and proof of destruction provided to Ally.

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 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

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

8.5.3.1.2. • Other industry-based best practices that are not deprecated (NIST SP 800-131A Rev. 2)

8.5.3.2. Asymmetric (Public Key) Ciphers

8.5.3.2.1. • Rivest-Shamir-Adleman (RSA)

8.5.3.2.2. • Minimum of 2048-bit Keys must be used for all systems

8.5.3.2.3. • Other industry based best practices that are not deprecated (NIST SP

800-131A Rev. 2)

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, including systems 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 (including authentication credentials) while in transit over any public shared network and non-wired network between Supplier and Ally, between Supplier and all external sources, and within Supplier network.

8.5.5. Secure encrypted transmissions must be used for all Non-Public Ally Data (including authentication credentials) while in transit over any public shared network and non-wired network between Supplier and Ally, between Supplier and all external sources, and within Supplier network.

8.5.6. All Ally Data stored by the Supplier that is classified by Ally as Confidential and comprises PII, PCI, or PHI, or that is classified by Ally as Secret, must be encrypted at all times.

8.6. **Identity and Access Management**

8.6.1. Supplier must ensure all user IDs, tokens or physical access badges are assigned to a unique Supplier employee or Subcontractor.

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

8.6.3. Supplier 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. Supplier 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. Supplier must ensure systems that support access to Non-Public Ally Data always requires the following password construction requirements:

8.6.5.1. Minimum length: 8 characters

8.6.5.2. Complexity: Must contain at least three of the following four characters: number, uppercase letter, lowercase letter, printable special character

8.6.5.3. History (reuse): > 6 passwords

8.6.5.4. Expiration: For all end-user accounts <= 90 days; privileged user accounts, including system administrators, 30 days; service account passwords must be changed at least annually

8.6.5.5. Failed login attempts: <= 6 attempts

8.6.5.6. Account lockout: Accounts must remain in locked status 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.

8.6.5.7. 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. Supplier must ensure that systems used to access Non-Public Ally Data or Ally Systems 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. Supplier must change its passwords immediately whenever it is believed that an account may have been compromised.

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

8.6.6.4. 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.

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

8.6.6.6. 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. Supplier must ensure procedures exist for prompt modification or termination of access or rights in response to organizational changes.

8.6.9. Supplier must immediately notify Ally if a Supplier's employee or subcontractor with access to Ally Data or Ally Systems is terminated, or not working on the Ally account. All account permissions must be updated on Suppliers 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. Supplier must ensure procedures exist for appropriate provisioning, management, and deprovisioning of privileged accounts.

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

8.6.12. If a Supplier requires remote access to Ally Data or Ally Systems, that Supplier must always use an Ally approved method.

8.6.13. Any internet applications or services hosted at Supplier sites that provide Ally prospects or customers with a website, mobile or tablet app to support a product or service must have an authentication process that complies in all material respects with the requirements of the FFIEC's 2005 guidance entitled Authentication in an Internet Banking Environment as well as its 2011 Supplement entitled Supplement to Authentication in an Internet Banking Environment.

8.6.14. Supplier is required, by the commencement of the provision of Services to Ally, to provide an authentication process that complies with these Requirements.

8.6.15. Without limiting anything set forth in these Requirements, if during the term of the Agreement, the Supplier's authentication process does not comply with applicable laws or regulations, the Supplier 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. 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 Supplier's 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 Supplier may agree to an alternative solution if

such terms and costs are mutually agreed to.

8.7. **Monitoring, Response, and Recovery**

8.7.1. Supplier must have a documented plan and associated procedures for response to an information security event. 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. Supplier must notify Ally of all information security incidents in accordance with the requirements of the Agreement.

8.7.5. Once the Supplier discovers or is notified of an information security incident, it must investigate, fix, restore, and conduct a root cause analysis.

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

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

8.7.8. If Ally is not satisfied with speed or effectiveness of investigation, Supplier must include Ally information security staff in the investigation and response teams.

8.7.9. Supplier 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.

8.7.10. Supplier 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. Supplier 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. Supplier must ensure that all IT Systems and applications that are used to store, process, and/or transmit Non-Public Ally Data, and are accessible via the Internet are only accessible and accessed via the Supplier's 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 (firewall, web application firewall, reverse proxy, etc.) allowing only the specific hosts, protocols and services required to provide the functionality.

8.8.5. Firewall rules, router access control lists (ACLs), IP Whitelists, or other access lists must be reviewed and updated every six months.

8.8.6. Supplier must have an intrusion detection system (IDS), or intrusion prevention system (IPS), or equivalent network and host monitoring in place to monitor, detect and protect connections to their network where Ally Non-Public Data is stored, processed, maintained, or transmitted.

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

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

8.8.9. Wireless networks that support access to Non-Public Ally Data, including back office wireless networks must be encrypted with current encryption algorithms. Use of weak, flawed, or insecure algorithms are not allowed.

8.8.10. Internet applications and services hosted at Supplier sites that provide Ally prospects or

customers with a website, mobile, or tablet app to support a product or service must meet the compliance requirements within Section 8.6.

8.8.11. Supplier 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 or Ally Systems.

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

8.8.13. On workstations being used to access Non-Public Ally Data, end users must not be permitted to have local administrative access. Key workstation security settings (e.g., screen saver, antivirus) must be unalterable by end users. Workstations must be configured to prevent ability to copy Non-Public Ally Data from workstations to peripheral devices (e.g., CD, DVD, USB drives).

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

8.9. Vulnerability Management

8.9.1. Supplier must have, maintain, and follow a documented process to protect all IT Systems that process, store, maintain or access Ally Data or Ally Systems from known security vulnerabilities by installing applicable vendor supplied security patches in a timely manner based on the risk. All critical security patches must be applied within one week of their release.

8.9.2. Supplier must ensure malware, virus, trojan, and spyware protection is deployed on all IT Systems used to access Ally Data or Ally Systems and have the most recent manufacture's signatures, definition files, and security updates.

8.9.3. Suppliers 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 Data must be covered as part of the scope of the tests.

8.9.4. Suppliers with access to Non-Public Ally Data must also ensure that infrastructure, network, and application security vulnerability assessments 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.

8.9.5. Any vulnerabilities identified must be remediated within the following timeframes: Critical: 7 days - High: 30 days - Medium: 60 days - Low: 180 days.

8.9.6. All Suppliers must provide Ally with evidence that supports completion of security vulnerability assessments and prompt remediation on at least annual basis. Suppliers deemed critical by Ally 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:

- Detailed 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)
- Attestation from Supplier's senior leadership affirming completion of vulnerability assessments and timely remediation.

9.0. Privacy Standards

Ally requires that if Supplier has access to Ally Data, including any Confidential Information or Consumer Information, Supplier 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.

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

9.3. Have documented data management procedures addressing the following:

- 9.3.1. Data usage, collection, and sharing (including Privacy Notice communications if Consumer Information is subject to sharing)
- 9.3.2. Data storage, retention, and deletion/destruction
- 9.3.3. Data quality and integrity
- 9.3.4. Data inventory and classification
- 9.3.5. Data collection methods (paper and electronic)

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

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

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

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

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

9.7. 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 Suppliers and Suppliers 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 Suppliers and Suppliers 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 Suppliers and Suppliers 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 Suppliers and Suppliers 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 Suppliers to identify, track, and treat issues that arise from a control failure.

10.1.4. **General Compliance Training**

Ally requires Suppliers to have a documented, sustainable, and repeatable, compliance-specific training policy to include role-related employee training and testing/attestation on a specified cadence.

10.2. **Anti-Corruption**

10.2.1. Ally requires that its Suppliers, Supplier employees, and Subcontractors demonstrate integrity at all times and comply with Anti-Corruption Laws.

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

10.2.3. Anti-Corruption Laws prohibit payments through intermediaries (e.g., vendors, suppliers, 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 Supplier employee with knowledge that the Subcontractor or Supplier 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 Supplier 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 Supplier'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, Supplier must escalate such transaction or activity to Ally via the Ally Ethics Hotline at 800-971-6037.

10.2.5. Ally requires Suppliers 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-Briary and Facilitation of Payments compliance violations.

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

10.3.1. If Supplier 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), Supplier 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 Supplier 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; Supplier 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)**

Generally, Suppliers conducting services for Ally will ensure they either follows 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**

10.5.1.1. Ally requires Suppliers 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.

10.5.1.2. Ally requires Suppliers 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.

10.5.2. **Consumer Complaints**

Ally requires Suppliers that interact with Ally customers to have a risk-based documented, repeatable, and sustainable complaints management system in place to handle consumer complaints received with respect to Ally services.

10.5.3. **Fair Lending**

10.5.3.1. Ally requires Suppliers 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.

10.5.3.2. Ally requires Suppliers that provide any service related to any aspect of the credit lifecycle (e.g., sales, marketing, credit applications, call center, collections, repossessions) to have documented Fair Lending training and evidence of completion.

10.6. **Licensing Oversight**

Ally requires Suppliers that provide Services that are required by Applicable Law to be performed by licensed agents on Ally's behalf to have a documented, sustainable, and repeatable licensing compliance program, process, or procedure intended to ensure required licenses held by individuals and the company are obtained before engaging in support for Ally and maintained while providing services for Ally.

10.7. **PCI Compliance**

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

10.7.2. Ally requires Supplier to maintain a Data Flow Diagram.

10.8. **Financial Transactions**

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

11.0. Business Continuity Standards

Business Continuity Planning (BCP) 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. Supplier 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 Supplier's business continuity obligations in the Agreement, the following standards provide direction for the development and implementation of business continuity plans to mitigate the impact to Ally of a Supplier business disruption in the event under the Agreement one was to occur.

11.2. These Business Continuity Standards are specifically designed to align with Federal Reserve Board (FRB) and Federal Financial Institutions Examination Council (FFIEC) guidance.

11.3. **BCP Framework**

To maintain effective business continuity, and while performing Services to Ally, Supplier must implement the following Business Continuity Planning framework:

- Business Impact Analysis/Assessment (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

11.3.1. **Business Impact Analysis/Assessment (BIA)**

The BIA is a management level process that uses a consistent methodology to measure the quantitative (e.g., financial revenue loss, incurred expenses) and qualitative (e.g., operational customer or reputational impacts, legal or regulatory impacts, work backlog) risk exposure to Supplier resulting from a business disruption. The BIA takes into consideration escalating losses over time. BIAs must be reviewed and updated annually to ensure Supplier has current data to support risk-based business continuity planning and the alignment of recovery strategies.

11.3.2. **BCP Site Risk Assessment**

The BCP Site Risk Assessment determines threat impacts and prioritizes scenarios based upon practical experiences, potential circumstances that could disrupt work areas, business processes, facilities, or geographic locations in order to enhance response capabilities. BCP Site Risk Assessments must be periodically reviewed and updated to prioritize event and incident scenario impacts by identifying the likelihood of occurrence and the potential magnitude of the impact to Supplier and its ability to meet internal and external customer expectations.

11.3.3. **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.

11.3.4. **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.

11.3.5. **Crisis Management/Incident Response Plan (CMP/IRP)**

Crisis Management/Incident Response defines the overarching structure supporting crisis management and continuity of operations across Supplier. Supplier should develop and implement the following:

11.3.5.1. Crisis Management Plan

The CMP documents processes and practices to safeguard employees and minimize the impact of emergencies (e.g., fires, natural disasters, terrorism) or other incidents or crises (e.g., significant frauds, lost utilities, security breaches). The CMP must be reviewed and updated at least annually to ensure Supplier has corporate-wide crisis management response procedures that incorporate and align all aspects of the response from immediate, tactical emergency response to executive strategic decision-making on critical business, financial, and policy issues.

11.3.5.2. Pandemic Plan

The Pandemic Plan focuses on awareness, prevention/preparedness and response/recovery for a pandemic situation that incorporates guidance from the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC). The Pandemic Plan must be reviewed and updated at least annually to ensure Supplier employees are provided with a corporate-wide escalation plan based on the impact of a pandemic event on Supplier's staff, facilities, and customer service levels.

11.3.5.3. Incident Response Plan (IRP)

IRPs are designed to establish accountability (decision-making authority), lines of communication, and protocols necessary to manage an incident that may or may not result in a business or system disruption. Supplier must develop, implement, and review/update their IRPs at least annually to enable a coordinated and timely response to an incident as it unfolds.

11.3.5.4. Crisis Communications Plan

Crisis Communications Plans establish close collaboration and communications to facilitate timeliness and consistency in the message sent to interested parties internally and externally during a crisis. The Plan should include communication channels available during both work and non-work hours, including alternate communications between Supplier and Ally.

11.3.5.5. Emergency Response Plan (ERP)

Emergency Response Plans (ERPs) document immediate, site-specific actions to protect health and safety, as well as physical assets. ERPs must be created and reviewed/updated at least annually to ensure Supplier can rely upon Supplier's specific protocols and trained responders to promptly mitigate and help resolve an event.

11.3.6. **Plan Exercising and Testing**

The effectiveness of BCP is validated through an ongoing schedule of exercising/testing of BRPs, IT DRPs, and CMPs/IRPs, 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 strategy is viable and executable. Testing and certification of Supplier's contingency and disaster recovery plans must occur at least once every calendar year during the Term.

11.3.7. **Subcontractor Management**

Conduct Business Continuity Planning, as well as regular monitoring and testing of controls, to appropriately understand Subcontractor(s) compliance with their obligations under the Agreement including these Requirements.

12.0. Physical Security Standards

Supplier must adhere to the following physical security standards at all Supplier facilities when 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

Supplier 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 Suppliers 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 Supplier allow anyone to enter a restricted area by following another 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 Supplier.

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

12.2.3. Supplier and authorized Visitors must visibly display credentials at all times while on the property of any Supplier facility. Visitor credentials must be visibly different than Supplier credentials.

12.2.4. Visitor Access Controls: The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:

- 12.2.4.1. All Visitors are to remain in the entry lobby or reception area until the host arrives to escort the Visitor.
- 12.2.4.2. All Visitors must present a valid (unexpired) government issued photo ID when signing in.
- 12.2.4.3. All Visitors must sign in and out on a Visitor log providing name, company represented, date, in and out time, and person being visited.
- 12.2.4.4. Supplier receiving the Visitor is responsible for ensuring the Visitor is escorted at all times while at facility.
- 12.2.4.5. Visitor logs must be maintained for audit and review for no less than 90 days.
- 12.2.4.6. Physical access for Visitors must be limited to one access point, and signage must be posted to direct Visitors to the appropriate location.
- 12.2.4.7. Supplier and authorized Visitors must be prohibited from admitting unauthorized Visitors through any other access point or without following Visitor access control

procedures.

12.2.4.8. 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.

12.2.5. Physical Electronic Access Control Systems Controls: The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:

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

12.2.5.2. 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.

12.2.5.3. When a physical electronic access control system is utilized, each Supplier 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.

12.2.5.4. 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.

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

12.2.5.6. Suppliers who terminate employment or have employment terminated must have their access removed immediately.

12.2.6. Physical Intrusion Alarm Controls: Suppliers who store Confidential Information or Consumer Information must operate and maintain an alarm /alerting system that notifies responsible and responding forces when and where an immediate response is required (e.g., duress alarms, intrusion alarms, door open over-ride notices).

12.2.7. 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.

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

12.2.9. 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).

12.2.10. 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.

12.2.10.1. 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.

12.2.10.2. PIN codes, passcards, or any unique identifier that allows for arming/disarming of an intrusion alarm may not be shared.

12.2.10.3. PIN codes, passcards, and other unique identifiers must be managed appropriately, including disabling PINs and passcards upon a Supplier's separation.

12.2.11. Access Card and Physical Key Controls: The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:

12.2.11.1. Each facility must control and monitor the number of access cards and/or physical keys issued.

12.2.11.2. 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.

12.2.11.3. A record of the physical key number, name of the holder, and signature of the holder

must be maintained for all physical access keys issued or returned. At any given time, the log must accurately reflect the location of all physical access keys.

12.2.11.4. Key records may be held electronically in an access control software system, provided the system is able to capture the signature of the key holder.

12.2.11.5. 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.

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

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

12.2.12. High-Security Area Controls: The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:

12.2.12.1. A physical electronic access control system must be used to secure and track entrance to the High Security Area.

12.2.12.2. A monthly audit of authorized individuals must be conducted for all High-Security Areas.

12.2.12.3. Those who no longer have the need for regular access to High-Security Areas should have their access removed immediately.

12.2.12.4. Results of the audit must be maintained for at least three years.

12.2.12.5. All Visitors to a High-Security Area must have a pre-approved purpose for entering the area, must be escorted by an authorized Supplier 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.

12.2.12.6. Visitor logs for High-Security Areas must be accessible and available upon request for at least one year.

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

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

12.2.12.9. Data Centers: In addition to requirements for High Security Areas, the following must be implemented and enforced in Data Centers operated by Supplier in facilities where Confidential Information or Consumer Information is stored:

12.2.12.9.1. 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.

12.2.12.9.2. Utilize dual factor authentication for entry.

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

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

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

12.3.1. 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).

12.3.2. 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.

12.3.3. The placement of video surveillance at a facility adheres to clear, documented security objectives (e.g., command, control, response, or investigative).
12.3.4. All video surveillance systems must be recorded using digital technology that can be remotely monitored.
12.3.5. Each facility equipped with video surveillance technology is responsible for confirming that all cameras are functional by testing (i.e., viewing live images) on a daily basis. Documentation of testing must be recorded for audit.
12.3.6. Each facility equipped with video surveillance technology is responsible for confirming the system is recording and retaining video from each camera by testing at least once per week. Documentation of testing must be recorded for audit.
12.3.7. Video surveillance recording equipment will be capable of retaining video for a minimum of 30 days for review. Where Payment Card Industry (PCI) data is protected, recordings must be maintained for no less than 90 days.
12.3.8. All video surveillance cameras must be overt and visible. Covert video monitoring as part of a physical security program is not permitted.

12.4. **Reliability of Physical Security Infrastructure**
The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:
12.4.1. Supplier must regularly review that any associated equipment (either installed and maintained by the Supplier, Subcontractor, or by any other third party such as a landlord or Third Party data center) is properly functioning and in good working order.
12.4.2. All applicable electronic physical security controls must be connected to an uninterruptable power supply.

12.5. **Photographic and Recording Equipment Standards**
The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:
12.5.1. Supplier 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.

12.6. **Contract Security Management**
The following must be implemented and enforced by the Supplier in facilities where Confidential Information or Consumer Information is accessed, transmitted, processed, or stored in the provision of Services during the Term:
12.6.1. Standard operating procedures or post orders must be developed for any facilities(s) with a contract or proprietary security force.
12.6.2. Post orders must be written with the intent to support the day-to-day monitoring and maintenance of the physical security program.
12.6.3. Daily activity reports and incident reports must be a part of the post orders.
12.6.4. Reports must be maintained for three years.

13.0. **Subcontractor Management**

As a regulated financial institution, Ally is expected to identify and understand the services of any Subcontractor. In addition, Ally requires that Suppliers have a proper risk based Third Party Risk Management Program in place to oversee these Subcontractors in a similar manner that Ally oversees our Third Parties. Ally requirements align to FRB Guidance for Managing Outsourcing Risk (FRB SR13-19a).

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

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