DATA PROTECTION EXHIBIT

This Data Protection Exhibit ("**Exhibit**") shall be incorporated into the Mutual Confidentiality and Non-Disclosure Agreement between Vendor and Regions (the "**NDA**") and describes the privacy, data protection, information security, and cybersecurity requirements applicable to all of the products and services and other materials, information, data, and reports developed for or delivered to Regions by or on behalf of Vendor and/or one of more of its Affilliates under one or more Contracts ("**Deliverables**"). Capitalized terms used in this Exhibit and not otherwise defined herein have the meanings given to them in the NDA.

DEFINITIONS

Definitions. The following terms have meanings ascribed to them when used in this Exhibit:

a. "**Applicable Data Protection Law**" means any applicable privacy, security, or other related Legal Requirement that protects Regions' Protected Information or Regions' Systems or relates to Processing. Such Legal Requirements may include but are not limited to: (i) federal or state data protection or privacy laws or regulations, including the California Consumer Privacy Act and California Privacy Rights Act; (ii) federal or state cybersecurity laws or regulations, including the New York Department of Financial Services Cybersecurity Rule; (iii) the Health Insurance Portability and Accountability Act of 1996, to the extent applicable to the Deliverables; (iv) the Gramm-Leach-Bliley Act; (v) the Federal Reserve Interagency Guidelines Establishing Information Security Standards for banking institutions; (vi) the Fair Credit Reporting Act; (vii) the Payment Card Industry (PCI) Data Security Standard, to the extent applicable to the Deliverables; and (viii) any other federal, state, or industry law, regulation, or binding guidance which exists currently or which may exist in the future and which applies to the Deliverables provided under the Contracts.

b. "**Consumer Request**" means: (i) any inquiry by an individual about how to submit a request, or the status of a pending request, with respect to any Personal Data Processed under the Contracts; or (ii) any other request that seeks information or asserts rights available under Applicable Data Protection Law. Consumer Requests include, but are not limited to, opt-out requests, requests for access, correction, portability, or deletion, and requests to identify or provide details regarding Personal Data Processed.

c. "**Industry Standard(s)**" means the then-current version of, as applicable: (i) the National Institute of Standards and Technology ("**NIST**") publications related to privacy, information security, and cybersecurity (including, without limitation, NIST SP 800 Series publications and the NIST Privacy Framework); (ii) International Organization for Standardization and International Electrotechnical Commission ("**ISO/IEC**") 27001 and related guidance and standards; (iii) Escal Institute of Advanced Technologies, Inc. ("**SANS**") standards and publications; or (iv) any substantially similar and related standards or guidance which are regularly referenced or relied upon by financial services and technology industries for privacy, information security, or cybersecurity controls, policies, and procedures designed to safeguard data.

d. "**Information Assets**" means Protected Information in any form, whether electronic, hardcopy, photographic image, microfiche or microfilm or in digital, magnetic, optical or electronic form, and all Systems which Process Protected Information.

e. "**Information Security**" means cybersecurity, technical, physical, organizational, administrative, and other safeguards, controls, measures, and processes for the protection against the loss or compromise of the security, confidentiality, integrity, or availability of Information Assets.

f. "**Information Security Event**" means: (i) any circumstance pursuant to which Applicable Data Protection Law requires notification to be given to affected parties, interested parties (including Governmental Authorities, or officials), or other activity in response to such circumstance; (ii) any actual, threatened, or reasonably suspected or foreseeable circumstance that compromises, or could reasonably be expected to compromise, Information Assets in a fashion that either does or could reasonably be expected to permit unauthorized Processing of any Protected Information; (iii) any act or attempt, successful or unsuccessful, to Process or prevent Processing of Information Assets that is, in whole or in part, illegal or not authorized by Regions; (iv) any ransomware (*e.g.*, encrypting or crypto-ransomware, locker ransomware, Master Boot Record ("**MBR**") malicious code, mobile device ransomware, IoT ransomware, or a similar type of application, code or software) attack on Information Assets; or (v) any event meeting the definition of a "Notification Incident", as stated in 12 C.F.R. Part 53. Notwithstanding the foregoing, an "Information Security Event" shall not include

trivial and routine incidents such as port scans, pings, and other broadcast attacks, so long as they do not materially affect the security, confidentiality, integrity, or availability of the Information Assets.

g. "**Information Security Event Response Plan**" means the collection of written policies, standards, procedures, practices, and controls designed and implemented by Vendor to detect, manage (including appropriate remediation), and resolve Information Security Events.

h. "**Information Security Program**" means the collection of written policies, standards, procedures, practices, and controls implemented by Regions or Vendor to protect the security, confidentiality, integrity, and availability of Information Assets.

i. "**Information Security Vulnerabilities**" means a temporary or permanent condition or state of an Information Security Program or any aspect thereof, whether related to design, implementation, maintenance or otherwise, that could be reasonably expected to permit, facilitate, or result in an Information Security Event.

l. "**Personal Data**" means personally-identifiable information or data, including biometric information, as such information or data is defined by or regulated by Applicable Data Protection Law.

m. "**PHI**" shall mean "Protected Health Information" as such term is defined in Section 160.103 of the Health Insurance Portability and Accountability Act of 1996 as codified at 45 C.F.R. Subtitle A, Subchapter C, Part 160 *et seq.* as amended.

n. "**Process**", "**Processed**", or "**Processing**" means and includes any access to, or any collection, receipt, use, manipulation, disclosure, sharing, transmission, disposal, maintenance, or storage of, data or information or Systems storing or accessing such data or information. "Process" includes such activities when performed by or within the environment of SaaS or cloud computing environments.

o. "**Protected Information**" means data and information, in any form or medium, that are subject to Applicable Data Protection Law and Processed by Vendor, which includes but is not limited to Sensitive Business Information, Confidential Information, Personal Data, PHI, and to the extent applicable, Payment Card Industry ("PCI") data ("PCI Data").

p. "**Regions Information Assets**" means Information Assets: (i) belonging to or under the custody, supervision, or control of Regions; (ii) provided or made available by Regions or its designee to Vendor; (iii) Processed by Vendor on behalf of Regions including any derivation or modification thereof; or (iv) any information generated as a result thereof.

q. "**Requirements**" means the obligations and conditions stated herein, including the Minimum Cybersecurity Requirements set forth at https://www.regions.com/-/media/pdfs/about-regions/Minimum-Cybersecurity-Requirements.pdf, which are expressly incorporated herein and which are applicable to Vendor and the Deliverables provided under the Contract. In the event of any ambiguity or conflict between the Requirements and Legal Requirements regarding any control or safeguard described and applicable to the Deliverables, then the Legal Requirements shall control.

r. "**Sensitive Business Information**" means the non-public, business-related information of Regions that, if Processed without authorization or in violation of the Requirements, is reasonably likely to cause a material adverse impact on the business, operations, or security of Regions.

s. "**System(s)**" means all (i) computer, electronic or telecommunications systems, or resources of any variety (including, but not limited to, personal computers, laptops, workstations, servers, network devices, portable storage devices, electronic storage media, cabling, databases, hardware, software, storage, telephone switching, environmental control, industrial/process control, private branch exchanges, cloud services, interconnection devices and mechanisms, and other computing and infrastructure equipment) that Process electronic information, (ii) networks of which such systems in (i) above are a part or communicate with, and (iii) are used directly or indirectly by Vendor or in connection with providing Deliverables to Regions.

t. "**Vendor**" shall have the meaning given to that term in the NDA, and for purposes of this Exhibit shall include Subcontractors or Personnel that Processes or has the ability to Process Regions Information Assets.

DATA PROTECTION REQUIREMENTS

2. Processing of Protected Information. The following provisions apply to Vendor and the Deliverables:

a. Limited Use and Minimum Necessary. Vendor will provide the same level of protections as required by, and only Process Protected Information in accordance with, Applicable Data Protection Law and the terms

of the Contract. In addition, Vendor shall only Process Protected Information to the extent necessary to provide the Deliverables. If and to the extent Regions is currently or subsequently designated under Applicable Data Protection Law or other applicable law as a controller, processor, fiduciary, data fiduciary or is otherwise mandated to impose additional limitations on the use or Processing of Protected Information ("Mandatory Use Restrictions"), Regions shall inform Vendor of such designation and the applicable Mandatory Use Restrictions in writing, as may be amended from time to time. Vendor shall be bound by and shall follow the Mandatory Use Restrictions as communicated by Regions.

b. Access Limitations. Vendor will limit access to Protected Information to, and will share information with, only those Persons who have a legitimate need to access such Protected Information to provide the Deliverables. Vendor will instruct all such individuals in writing as to the obligations set forth in this Exhibit, require such individuals' compliance with the obligations set forth in this Exhibit, and shall be responsible therefor.

c. Sale of Protected Information. Vendor will not sell any Protected Information to any third party. For purposes of this Exhibit, "sell" (and similarly defined words such as "sale") is as defined under Applicable Data Protection Law.

d. Sharing of Protected Information. Vendor will not share any Protected Information with any third party for marketing purposes, including cross-context behavioral advertising.

e. Geolocation Restriction. Vendor shall not Process any Regions Information Assets outside of the United States without Regions' prior written consent, which may be withheld in Regions' sole discretion.

f. GAI Restriction. Vendor shall not utilize generative artificial intelligence ("**GAI**") (including without limitation, ChatGPT, Jasper.ai, OpenAI, DALL-E, or any other substantially similar technologies) to (i) Process Regions Information Assets and/or (ii) provide any Deliverables without the prior written approval of Regions.

3. Use of Subcontractors. Nothing in this Exhibit modifies any limitation on Vendor's use of Subcontractors, or any rights of Regions to audit or participate in an audit of Vendor's Subcontractors, to the extent such rights are present in the Contracts. Wherever Vendor is permitted and uses Subcontractors in the provision of the Deliverables, Vendor will maintain due diligence policies and procedures to require that such Subcontractors agree in writing to terms no less stringent than those set forth in this Exhibit and adhere to the Requirements stated herein. Vendor will remain fully responsible and liable to Regions for compliance of its Subscontractors with the obligations set forth in this Exhibit.

4. Mandatory Disclosure of Protected Information. If Vendor is compelled or ordered by Governmental Authority which has jurisdiction over either of the Parties and subject matter referenced in this Exhibit to disclose any Protected Information (a "Production Request"), then unless prohibited by law or the order, Vendor shall notify Regions not less than ten (10) business days prior to the production date of the Production Request to permit Regions to object to the disclosure or seek an appropriate protective order or other remedy. Vendor shall, at its own cost, exercise commercially reasonable efforts to limit any such disclosure, to preserve the confidentiality of the Protected Information that will be disclosed, and cooperate with Regions with respect to any action taken concerning a Production Request, including seeking to obtain an appropriate protective order or other relief. If a remedy acceptable to Regions is not obtained by the date that Vendor must comply with the Production Request, then Vendor shall furnish only the minimum amount of Protected Information it is legally required to furnish.

5. Consumer Requests.

a. If Vendor receives a Consumer Request, Vendor shall promptly, and at no additional cost to Regions, direct the inquiring party to Regions, or, but only to the extent required by law, respond to that request on its own and/or on Regions' behalf. Thereafter, Vendor will: (i) assist Regions in timely responding to any Consumer Requests and reasonably cooperate and facilitate Regions' timely authentication, recording, investigation, processing, execution, and resolution of all Consumer Requests; and (ii) securely provide any information requested by Regions that is responsive to a Consumer Request as soon as reasonably practicable, but in all cases within the shorter of: (a) five (5) business days, or (b) such other time if stated in the Contract(s).

b. Any other requests received by Vendor from individuals, including complaints related to the Processing of data under the Contract(s), but which inquiries or requests are not Consumer Requests, will be subject to the terms

of the Contract(s) or handled through Vendor's own internal business practices and are not subject to the terms of this Exhibit.

INFORMATION SECURITY REQUIREMENTS

6. Information Security Framework and Audits**.**
   - **a.** At all times while providing the Deliverables, Vendor shall implement and maintain an Information Security Program that meets the Requirements. In the event of any ambiguity or conflict between the Requirements and Industry Standards regarding any control or safeguard described and applicable to the Deliverables, then the Requirements shall control.
   - **b.** Vendor grants Regions, any Governmental Authority having oversight of Regions or its Affiliates, or any third-party auditor on Regions' behalf, permission to perform an audit or assessment of Vendor's compliance with the Requirements, including Business Continuity Plan ("**BCP**") and Disaster Recovery ("**DR**") materials, plans and test results at least annually. Regions shall have the right to perform penetration testing and vulnerability scanning of the Systems, including any hosted applications and infrastructure, upon at least thirty (30) days' notice to Vendor. In addition, Vendor grants Regions the right to conduct additional targeted audits ("**Targeted Audits**") in response to: (i) an Information Security Event; (ii) any unauthorized Processing of Protected Information; (iii) any identified material deviation from the terms of this Exhibit or an agreed-upon alternative compensating control; (iv) any material inaccuracy or misrepresentation made by Vendor about the controls and/or underlying risks applicable to Information Assets; or (v) following a man-made or natural disaster. The audits or assessments may be written or physical or as otherwise determined by Regions.
   - **c.** In addition to the audit rights stated herein, Vendor agrees to provide reasonable information promptly in response to Regions' requests related to vulnerabilities, zero-day exploits, or similar issues related to the privacy or security Requirements which are: (i) generally known, (ii) later discovered, or (iii) which are covered in industry alerts or media reports.
   - **d.** Where available, Vendor will furnish a copy of a current System and Organizations Controls 2, Type II report (Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy) or equivalent direct successor report (a "**SOC 2 Type II**"), including description of the trust services criteria or principles assessed, and any scope limitation under such report. Regions may, in its sole discretion, deem the audit requirement stated herein satisfied by any SOC 2 Type II report provided by Vendor, but only with respect to those controls assessed within the defined scope of the report. Regions may also, at its sole option, agree to accept an alternative third-party assessment or certification of Vendor's Information Security Program, such as a ISO27001 certificate (including the Statement of Applicability, or PCI-DSS Attestation of Compliance or HITRUST certification), in lieu of exercising its right (or some portion of that right) to audit, to the extent such certification relates to the Requirements. For clarification, and without limiting the foregoing, Regions reserves the right to conduct audits without relying on any Vendor or third party audit reports or certifications and also reserves the right to audit any Requirements that are not sufficiently addressed in any audit report or certification.
   - **e.** Where the parties reasonably and expressly agree in writing that any Information Security Program Requirement stated in this Exhibit is inapplicable or is unduly onerous in light of the Deliverables provided and the risks to Information Assets, then the parties will work together in good faith to determine whether appropriate alternative compensating controls may be used to meet the spirit and intent of the Requirements. In addition, if a Requirement is expressly waived by Regions entirely, then in all such cases, use of alternative compensating controls, or a waiver of a Requirement: (i) is subject to Regions' continuing consent in its sole discretion, which may be withdrawn, revoked, or conditioned at any time for any reason; and (ii) shall not be effective unless documented and agreed to in writing by Regions.

7. Network Security.
   - **a.** Regions may suspend or terminate any network or other remote connection with Vendor at any time in Regions' discretion and without warning.

b. Regions Protected Information must not exist on any computer or device that is exposed to the Internet or other non-Vendor network, unless Vendor has implemented appropriate Information Security safeguards for such computer or device that conform to the Requirements.

8. Information Security Event Response and Notification.
   a. For as long as Vendor Processes Protected Information, Vendor must maintain a documented Information Security Event Response Plan that complies with Applicable Data Protection Law and current Industry Standards.
   b. Vendor must maintain all records, evidence, and information regarding any Information Security Event and Vendor's response. Such record and evidence retention shall utilize chain of custody procedures, where applicable, and substantially conform to Industry Standards.
   c. Vendor has disclosed to Regions in writing any Information Security Event experienced by Vendor prior to the execution of the Contract if remediation of the cause(s) of the Information Security Event has not been fully implemented.
   d. Vendor shall report to Regions any Information Security Event involving Regions Information Assets immediately upon discovery, but in no event more than twelve (12) hours following its detection, via email to CISO@regions.com. Thereafter, Vendor will:
      i. Promptly furnish all details of the Information Security Event, including the date and means of discovery. Where it is not possible to provide all details of the Information Security Event at the time of initial reporting, Vendor shall provide as much information as possible in its initial report and thereafter shall provide additional information as soon as it becomes available;
      ii. Take immediate steps to contain and remediate the Information Security Event in accordance with Applicable Data Protection Law;
      iii. Cooperate with Regions in Regions' assessment of whether: (i) notice or other communication is to be provided to any third party; or (ii) any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Regions shall retain sole discretion regarding whether any communications to impacted parties (including Regulatory Agencies) which identify Regions is required and the content of such communication. Vendor shall not issue or publish any such communication without the express prior written consent of Regions;
      iv. Take remedial action to prevent a reoccurrence of any such Information Security Event;
      v. Cooperate fully with Regions (or Regions' representative or designee) in Regions' investigation of the Information Security Event or the Vendor or third parties related to the Information Security Event, including but not limited to providing Regions appropriate access to the facilities, Systems, hardware, software, data bases and operations affected, facilitating interviews with relevant parties and making available all relevant records, logs, files, and data (including the use of forensic investigative tools, as applicable);
      vi. Cooperate reasonably with Regions in any proceeding initiated, filed, or asserted by Regions against any third parties to protect Regions' rights and the rights of others, in Regions' sole discretion; and
      vii. Reasonably and promptly cooperate with Regions to ensure timely access to Regions Information Assets.
   e. Nothing herein shall prevent Regions from taking any actions it determines to be required by Legal Requirements, including notification to Governmental Authorities, as applicable.

GENERAL REQUIREMENTS

9. Compliance.
   a. At all times while providing the Deliverables, Vendor shall comply with the Requirements, Applicable Data Protection Law, and, if applicable, the current PCI Data Security Standard (DSS).

b. At Regions' request, at any time during the term of the Contract, Vendor agrees to certify in writing its compliance with Requirements and must notify Regions promptly in writing if at any time Vendor determines it cannot meet its obligations stated herein.

10. Injunctive and Other Relief. Vendor acknowledges that Vendor's breach of or failure to comply with the Requirements, including the unauthorized Processing of Regions Information Assets, may cause damages or harm to the business reputation of either or both Vendor and Regions, which damages or harm may be difficult to quantify or otherwise may result in irreparable harm, and, in any such event, Regions shall be entitled to seek injunctive or other appropriate equitable relief from a court of competent jurisdiction, in addition to any other remedies available at law or in the Contract.

11. Right to Cure and Termination. If Regions reasonably determines that Vendor is in material breach of any of the Requirements, Vendor shall cure any such breach within five (5) calendar days of Regions providing written notice to Vendor unless the Parties agree to a different period in writing ("**Cure Period**"); provided, however, that no such Cure Period is available to Vendor in cases where Regions reasonably determines, in its sole discretion, that the breach cannot practicably be cured. For the avoidance of doubt, this Cure Period is specific to any breaches or alleged breaches of this Exhibit. In the event (i) Vendor fails to cure within an available Cure Period, or (ii) where Regions has reasonably determined, in its sole discretion, that no such Cure Period is available, then Regions may terminate the Contract(s) immediately upon written notice for cause and without any further opportunity for Vendor to cure the breach, and Regions shall have available any rights and remedies for termination for cause under any Contract as a result. In addition, Vendor shall reimburse Regions for all direct costs associated with such breach and termination (including, if applicable, the costs of the audit identifying such breach) and waive any penalties, fees, or damages associated with terminating the Contract. Nothing contained in this section shall waive any obligations of Vendor, under any Contract, related to continuity of performance or transition assistance.

12. Indemnification. Notwithstanding any limitations or exculpatory provisions contained in any Contract, for the subject-matter described herein, Vendor shall, at its sole cost and expense, defend, indemnify, and hold harmless Regions, its Affiliates, and all of their directors, officers, personnel, employees, agents, and contractors and their successors and assigns (collectively, "**Indemnitees**") from any and all expenses, damages, judgments, awards, settlements, losses, obligations, fines, payments, penalties, and liabilities (including, but not limited to, attorneys' fees, court costs, and other costs and expenses,) that an Indemnitee suffers, sustains, or incurs arising out of or in connection with any and all claims, actions, demands, complaints, suits, regulatory actions and causes of action (a "**Claim**"): (i) arising out of or relating to any Information Security Event; or (ii) arising out of or relating to Vendor's breach of the Requirements or other obligations set forth in this Exhibit. The obligations in this section shall be in addition to, and not in lieu of, any obligations, including but not limited to defense and/or indemnification obligations in the Contract(s) between the Parties. Further, the obligations in this section shall survive any termination or expiration of the Contract(s). Notwithstanding anything in any Contracts and for avoidance of doubt, the following shall constitute direct costs and damages to be indemnified by Vendor to Regions in connection with an Information Security Event and/or Vendor's breach of the Requirements or other obligations set forth in this Addendum: (i) notification costs; (ii) incremental fraud losses or reimbursements; (iii) identity theft restoration costs for affected employees or customers; (iv) costs of providing twelve (12) months (or any longer amount required by law) of fraud and credit monitoring services and identity theft insurance to affected employees or customers; (v) costs of re-issuing account credentials/cards to affected customers; (vi) three months of contact center operations from the date of discovery of the breach or Information Security Event; (vii) public relation costs; (viii) cyber extortion costs and/or payments; (ix) data recovery costs; (x) costs and expenses for internal and external breach remediation plans; (xi) damages, fines, fees, assessments, penalties or settlements with payment network operators or Regulatory Agencies arising out of or related to the breach or Information Security Event; and (xii) costs, including legal and other expert fees, associated with investigation of the breach or Information Security Event, including forensic investigations, root cause analysis, and potential remediation. It is specifically understood and agreed that any limitations of liability in any Contracts shall not apply to claims for breach committed by the Vendor or any Vendor Personnel of its obligations hereunder with respect to Regions' Confidential Information, including any breach of the terms and provisions of the NDA, or to the defense and indemnification obligations of the Vendor contained herein.