Branch Data Processing Addendum

1. Introduction

This Branch Data Processing Addendum ("**Addendum**") is an integral part of Branch Metrics, Inc.'s Terms & Conditions (or instead, where there is an existing service agreement in place between Customer and Branch prior to the effective date of this Addendum, (the "**Service Agreement**"), of that Service Agreement), which together with one or more Order Forms and exhibits, form the "**Agreement**" between Branch Metrics, Inc. ("**Branch**") and the Customer who agreed to and is party to the Terms & Conditions or Service Agreement ("**Customer**"), and is made part of the Agreement. This Addendum governs the manner in which Branch shall Process Customer Personal Data on behalf of Customer (who is Controller of the data subject to this Addendum) and only applies to the extent Branch serves as a Processor of such Customer Personal Data on behalf of Controller. This Addendum shall be effective on the date agreed to by Customer and will automatically terminate upon expiration or termination of the Agreement. Except for the changes made by this Addendum, the Agreement remains unchanged and in full force and effect. In the event of a conflict between the Agreement, including Order Forms and exhibits, and this Addendum, this Addendum shall control. The parties agree that this Addendum shall replace any existing data processing addendum the parties may have previously entered into in connection with the Branch Services. Capitalized terms have the meaning given to them in the Agreement, unless otherwise defined below.

2. Definitions

For the purposes of this Addendum, the following terms and those defined within the body of this Addendum apply.

a) "**Applicable Data Protection Law(s)**" means the relevant data protection and data privacy laws, rules and regulations to which the Customer Personal Data are subject. "Applicable Data Protections Law(s)" shall include, but not be limited to, the General Data Protection Regulation (EU 2016/679) (the "**GDPR**") and equivalent requirements in the United Kingdom including the Data Protection Act 2018 and the United Kingdom General Data Protection Regulation ("**UK Data Protection Law**"), and the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., including its regulations and the amendments made by the California Privacy Rights Act of 2020 ("**CCPA**") and privacy laws passed by other U.S. states (together with the CCPA, "**U.S. State Privacy Laws**").

b) "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. Controller is also a "business," as that term is defined in the CCPA.

c) "**Customer Personal Data**" means Personal Data pertaining to Customer's users received or collected by Branch, provided by Customer in its capacity as Controller to Branch, the Processor. The Customer Personal Data and the specific uses of the Customer Personal Data are detailed in Schedule 1 as required by the Applicable Data Protection Laws.

d) "**Personal Data**" shall have the meaning assigned to the terms "personal data", "personal information" or other similar terminology under Applicable Data Protection Law(s).

e) "**Process**," "**Processes**," "**Processing**," "**Processed**" means any operation or set of operations which is performed on data or sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.

f) "**Processor**" means a natural or legal person, public authority, agency or other body which Processes Customer Personal Data subject to this Addendum. Processor is also a "service provider," as that term is defined in the CCPA.

g) "**Security Incident(s)**" means the unauthorized access, use or disclosure of Customer Personal Data.

h) "**Sensitive Personal Data**" shall have the meaning assigned to the terms "sensitive personal information," "sensitive personal data," or "special categories of personal data" under Applicable Data

Protection Law(s) and shall include Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

i) **"Standard Contractual Clauses"** shall mean, only as applicable to Customer, (i) the UK Standard Contractual Clauses; and (ii) 2021 Standard Contractual Clauses.

k) "**Third Party(ies)**" means Branch-authorized contractors, agents, vendors and third-party service providers (i.e., sub-processors) that Process Customer Personal Data.

l) "**UK Standard Contractual Clauses**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses (available as of the effective date of this Addendum at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/), completed as set forth in this Addendum.

m) "**2021 Standard Contractual Clauses**" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914, completed as set forth in this Addendum.

3. Data Handling, Access and Processing

a**) Role of the Parties**. As between Branch and Customer, Customer is the Controller of Customer Personal Data, and Branch shall Process Customer Personal Data as a Processor acting on behalf of Customer, as to the Processing identified in Schedule 1.

b) **General Compliance by Branch**. Customer Personal Data shall be Processed by Branch to provide the Branch Services and otherwise in compliance with the terms of this Addendum and all Applicable Data Protection Law(s).

c) **General Compliance by Customer**. Customer agrees that (i) it shall comply with its obligations as Controller under Applicable Data Protection Law(s) in respect of its Processing of Customer Personal Data and any Processing instructions it issues to Branch, and (ii) it has provided notice and obtained (or shall obtain) all necessary consents (including without limitation, verifiable consent) and rights necessary under Applicable Data Protection Law(s) for Branch to Process Customer Personal Data and provide the Branch Services pursuant to the Agreement and this Addendum.

d) **Branch and Third Party Compliance**. Branch agrees to (i) enter into a written agreement with Third Parties regarding such Third Parties' Processing of Customer Personal Data that imposes on such Third Parties data protection and security requirements for Customer Personal Data that are compliant with Applicable Data Protection Law(s); and (ii) remain responsible to Customer for Branch's Third Parties' (and their sub-processors' if applicable) failure to perform their obligations with respect to the Processing of Customer Personal Data.

e) **Authorization to Use Third Parties**. To the extent necessary to fulfill Branch's contractual obligations under the Agreement or any Order Form, Customer hereby agrees that Branch's Affiliates may be retained as sub-processors, and Customer authorizes (i) Branch and Branch's Affiliates to engage Third Parties, including Amazon Web Services (hosting and data storage), Atlassian (processing of data subject requests), and Zendesk (Branch's data subject request portal), and (ii) Third Parties to engage sub-processors. Any transfer of Customer Personal Data shall comply with all Applicable Data Protection Law(s).

f) **Right to Object to Third Parties**. Branch (and/or its Affiliates) shall engage a new Third Party only after Branch has provided Customer with notification of a new Third Party. To receive notification via email regarding any new Third Party, Customer should email privacy@branch.io to request subscription to such notices. If Customer does not contact privacy@branch.io with any such request, Branch's posting of the name of such Third Party on its Third-Party List (available at https://branch.io/third-party-list) will be deemed to constitute notice of a new Third Party to Customer under this provision. Customer will have ten (10) calendar days to object after notice is given. In the event Customer objects within ten (10) calendar days after notice is given, Branch will make reasonable efforts to address Customer's objection. After this process, if a resolution has not been agreed to within ten (10) calendar days, Branch will proceed with engaging the Third Party. If Customer's reasonable objection remains unresolved, Customer will be given the opportunity to terminate the Branch Services for convenience without penalty as its sole and exclusive remedy or another such resolution as the

parties may agree. To the extent that Branch reasonably believes engaging a new Third Party on an expedited basis is necessary to protect the confidentiality, integrity or availability of Customer Personal Data or avoid material disruption to the Services, Branch reserves the right to give such notice as soon as reasonably practicable.

g) **Following Instructions**. Branch shall Process Customer Personal Data only in accordance with the documented instructions of Customer as specifically authorized by the Agreement or Processing to comply with other reasonable documented instructions provided by Controller (e.g., via email) where mutually agreed to by Processor and provided such instructions are consistent with and not in conflict with the terms of the Agreement. Branch will, unless legally prohibited from doing so, inform Customer in writing if it reasonably believes that there is a conflict between Customer's instructions and applicable law or otherwise seeks to Process Customer Personal Data in a manner that is inconsistent with Customer's instructions or Applicable Data Protection Law(s). The Agreement is Controller's complete and final documented instructions at the time of signature to Processor for the Processing of Personal Data.

h) **Confidentiality**. Any person authorized to Process Customer Personal Data must agree to maintain the confidentiality of such information or be under an appropriate statutory or contractual obligation of confidentiality.

i) **Personal Data Inquiries and Requests**. Branch agrees to comply with all reasonable instructions from Customer related to any requests from individuals exercising their rights in Customer Personal Data granted to them under Applicable Data Protection Law(s) ("**Privacy Request**"). Branch shall assist Customer in answering or complying with any Privacy Request by making available Customer Personal Data and technical processes to enable Customer to respond to any Privacy Request. If Branch receives a request from a Data Subject in relation to their Customer Personal Data, Branch will advise the Data Subject to submit their request to Customer, and Customer will be responsible for responding to any such request.

j) **Prior Consultation**. Branch agrees to provide reasonable assistance to Customer where, in Customer's judgement, the type of Processing performed by Branch is likely to result in a high risk to the rights and freedoms of natural persons (e.g., systematic and extensive profiling, or where the Processing uses new technologies) and thus requires a data protection impact assessment and/or prior consultation with the relevant data protection authorities.

k) **Demonstrable Compliance**. Branch agrees to keep records of its Processing in compliance with Applicable Data Protection Law(s) and provide such records to Customer upon reasonable request to assist Customer with complying with supervisory authorities' requests. Customer retains the right, upon notice, to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Personal Data, including any use of Customer Personal Data not expressly authorized in this Addendum.

l) **Processing of Certain Types of Personal Data**. Customer agrees that it shall not use the Branch Services to Process Sensitive Personal Data without Branch's explicit and prior written consent.

m) **Other Obligations**. Branch hereby certifies that it understands its restrictions and obligations set forth in the CCPA as well as in this Addendum, and will comply with those restrictions and obligations. Except as explicitly authorized by Applicable Data Protection Laws, Branch shall:

- not retain, use, or disclose Customer Personal Data outside of the direct business relationship between Customer and Branch that would render it a "Third Party" under applicable U.S. State Privacy Laws;
- not "sell" or "share" any Customer Personal Data, as such terms are defined in applicable U.S. State Privacy Laws, to any third party;
- not attempt to re-identify any pseudonymized, anonymized, aggregate, or de-identified Customer Personal Data without Customer's express written permission;
- comply with any applicable restrictions under Applicable Data Protection Law(s) on combining Customer Personal Data with personal data that Branch receives from, or on behalf of, another person or persons, or that Branch collects from any interaction between it and any individual;
- provide the same level of protection for Customer Personal Data as is required under Applicable Data Protection Law(s) applicable to Customer; and
- not otherwise engage in any Processing of Customer Personal Data that is prohibited or not permitted by "processors" or "service providers" under Applicable Data Protection Law(s).

4. International Data Transfer Mechanisms

Customer authorizes Branch and its Third Parties to transfer Customer Personal Data across international borders, including from the European Economic Area or the United Kingdom to the United States. Any cross-border transfer of Customer Personal Data subject to the GDPR or the UK Data Protection Law must be supported by an approved adequacy mechanism.

a) **UK Standard Contractual Clauses**:

i) General. The parties acknowledge and agree that to the extent that Branch Processes any Customer Personal Data under the Agreement, any related Order Forms, or exhibits, that are subject to the UK Standard Contractual Clauses, Branch and Customer hereby enter into the UK Standard Contractual Clauses for Controllers to Processors (and incorporated into this Addendum by reference). The UK Standard Contractual Clauses shall be interpreted in a manner consistent with the terms of this Addendum and Applicable Data Protection Law(s). To the extent that the terms of this Addendum directly contradict the UK Standard Contractual Clauses, the UK Standard Contractual Clauses will control.

ii) Application. The UK Standard Contractual Clauses will apply to (i) the legal entity that has executed this Addendum and entered into the UK Standard Contractual Clauses as a data exporter, and (ii) all Affiliates of Customer established within the United Kingdom, which have signed Order Forms for the Services. For purposes of the UK Standard Contractual Clauses, the aforementioned entities will act as the "data exporters" and Branch will act as the "data importer". The UK Standard Contractual Clauses shall be deemed completed as follows (with undefined capitalized terms meaning the definitions in the UK Standard Contractual Clauses):

(1) Table 1 of the UK Standard Contractual Clauses: (a) the Parties' details shall be the parties and their affiliates to the extent any of them is involved in such transfer, including those set forth in the Appendix of this Addendum; and (b) the Key Contact shall be the contacts set forth in the Appendix of this Addendum.
(2) Table 2 of the UK Standard Contractual Clauses: The Approved EU SCCs referenced in Table 2 shall be the 2021 Standard Contractual Clauses as executed by the parties.
(3) Table 3 of the UK Standard Contractual Clauses: Annex 1A, 1B, II, and III shall be set forth in Section 3(e) and the Appendix of this Addendum.
(4) Table 4 of the UK Standard Contractual Clauses: Either party may end this Addendum as set out in Section 19 of the UK Standard Contractual Clauses.
(5) By entering into this Addendum, the parties are deemed to be signing the UK Standard Contractual Clauses and its applicable Tables and Appendices.

b) **2021 Standard Contractual Clauses**:

i) General. The parties acknowledge and agree that to the extent that Branch Processes any Customer Personal Data transferred from the European Economic Union or Switzerland under the Agreement, any related Order Forms, or exhibits, outside the European Economic Area in a country that has not been designated as providing an adequate level of protection for Personal Data, including the United States, Branch and Customer hereby enter into the 2021 Standard Contractual Clauses for Controllers to Processors (and incorporated into this Addendum by reference). The 2021 Standard Contractual Clauses shall be interpreted in a manner consistent with the terms of this Addendum and Applicable Data Protection Law(s). To the extent that the terms of this Addendum directly contradict the 2021 Standard Contractual Clauses, the 2021 Standard Contractual Clauses will control.

ii) Application. The 2021 Standard Contractual Clauses will apply to (i) the legal entity that has executed this Addendum and entered into the Standard Contractual Clauses as a data exporter and, (ii) all Affiliates of Customer established within the European Economic Area or Switzerland, which have signed Order Forms for the Services. For purposes of the 2021 Standard Contractual Clauses, the aforementioned entities will act as the "data exporters" and Branch will act as the "data importer". Customer acts as a Controller and Branch acts as Customer's Processor with respect to the Personal Data subject to the 2021 Standard Contractual Clauses, and its Module 2 applies. With respect to the 2021 Standard Contractual Clauses:

(1) in Clause 7, the optional docking clause does not apply;

(2) in Clause 9, Option 2 applies; the time period for prior notice of Third Party changes will be as set forth in Section 3(f) (Right to Object to Third Parties) of this Addendum;
(3) in Clause 11, the optional requirement that data subjects be permitted to lodge a complaint with an independent dispute resolution body does not apply;
(4) in Clause 17 (Option 1), the 2021 Standard Contractual Clauses will be governed by Irish law;
(5) In Clause 18(b), disputes will be resolved before the courts of Ireland; and
(6) Annexes I and II of the 2021 Standard Contractual Clauses are set forth in the Appendix of this Addendum. Annex III is not applicable as the parties have chosen general authorization under Clause 9.
(7) By entering into this Addendum, the parties are deemed to be signing the 2021 Standard Contractual Clauses and its applicable Annexes.

c) **Revisions**. In the event that the European Commission or the United Kingdom requires the use of revised standard contractual clauses that are applicable to this Addendum, such revised standard contractual clauses shall automatically be deemed to replace the UK Standard Contractual Clauses or 2021 Standard Contractual Clauses, as applicable, without the need for any further action, unless otherwise agreed to by the parties.

d) **Termination**. The Standard Contractual Clauses shall automatically terminate once the Customer Personal Data transfer governed thereby becomes lawful under Applicable Data Protection Laws in the absence of such Standard Contractual Clauses on any other basis, and Branch has implemented any measures necessary to comply with such basis.

5. Information Security

Branch agrees to implement appropriate technical and organizational measures designed to protect Customer Personal Data as set forth in Annex II of this Addendum ("**Branch Information Security and Privacy Standards**"). Further, Branch agrees to regularly test, assess and evaluate the effectiveness of the Branch Information Security and Privacy Standards to ensure the security of the Processing. Customer acknowledges that the Branch Information Security and Privacy Standards may be updated from time to time to reflect process improvements or changing practices but the modifications will not materially decrease Branch's obligations as compared to those reflected in such terms as of the Effective Date.

6. Audits

Upon request from Customer, Branch agrees to reasonably cooperate with Customer for the purpose of verifying Branch's compliance with Applicable Data Protection Law(s). Upon Customer's request pursuant to Clause 9(c) of the 2021 Standard Contractual Clauses, Branch will provide the copies of the requested sub-processor agreements, and Branch may remove or redact all commercial or proprietary information or clauses beforehand to protect business secrets or other confidential information, and that such copies will be provided by Branch in a manner to be determined in its discretion, only upon request by Customer.

7. Return or Deletion of Data

Upon written request by Customer after Customer terminates use of all Branch Services, Branch shall delete or provide to Customer all Customer Personal Data in its possession or control, save that this requirement shall not apply to the extent Branch is required by applicable law to retain some or all of the Customer Personal Data, or to Customer Personal Data it has archived on back-up systems, which Customer Personal Data Branch shall securely isolate and protect from any further processing, except to the extent required by applicable law. The parties agree that the certification of deletion of Personal Data that is described in Clause 8.5 of the 2021 Standard Contractual Clauses shall be provided by Branch to Customer only upon Customer's request.

8. Security Incident

a) **Security Incident Procedure**. Branch will deploy and follow policies and procedures to detect, respond to, and otherwise address Security Incidents including procedures to (i) identify and respond to suspected or known Security Incidents, mitigate harmful effects of Security Incidents, document Security Incidents and their outcomes, and (ii) restore the availability or access to Customer Personal Data in a timely manner.

b) **Notice**. Branch agrees to provide prompt written notice without undue delay and within the time frame required under Applicable Data Protection Law(s) to Customer if it knows that a Security Incident has taken place. A delay in giving such notice requested by law enforcement and/or in light of Branch's legitimate needs to investigate or remediate the matter before providing notice will not constitute an undue delay. Such notice will include all available details required under Applicable Data Protection Law(s) for Customer to comply with its own notification obligations to regulatory authorities or individuals affected by the Security Incident.

9. Limitation of Liability

Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to the Agreement, whether in contract, tort or under any other theory of liability, is subject to the limitations of liability of the Terms & Conditions or Service Agreement (as applicable), and any reference in such section to the liability of a party means the aggregate liability of that party and all of its Affiliates under the Terms & Conditions or Service Agreement (as applicable). For the avoidance of doubt, Processor's total liability for all claims from the Controller and all of its Affiliates arising out of or related to the Agreement shall apply in the aggregate for all claims under Agreement, and, in particular, shall not be understood to apply individually and severally to Customer and/or to any Affiliate that is a contractual party to any such Agreement.

10. Severability

If any provision of the Addendum is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that the Addendum will otherwise remain in full force and effect and enforceable.

IN WITNESS WHEREOF, the parties have caused this Addendum to be signed by their duly authorized representatives effective as of the last date of execution below:

CUSTOMER:		**BRANCH METRICS, INC.:**	
Signature:		Signature:	
Name:		Name:	
Title:		Title:	
Date:		Date:	
App ID(s)*:			

Company Name:	

**You can find the App ID by visiting https://dashboard.branch.io/account-settings/app, under "App ID."*

Schedule 1 to the Branch Privacy and Security Addendum

1.1 Subject Matter of Processing	The subject matter of Processing is the Branch Services pursuant to the Agreement.
1.2 Duration of Processing	The Processing will continue until Branch's receipt of notification from Customer of termination of use of all Branch Services.
1.3 Categories of Data Subjects	Includes the end users of Customer's app(s) and/or websites into which the Branch SDK is integrated, and/or end users who click on Branch deep links.
1.4 Nature and Purpose of Processing	The purpose of Processing of Customer Personal Data by Branch is the performance of the Branch Services pursuant to the Agreement.
1.5 Types of Personal Data	The data collected via Branch's SDK and Branch links includes the following types of Personal Data: iOS Identifier for Advertising (IDFA) iOS Identifier for Vendors (IDFV) Android Advertising ID (GAAID) Android ID IP Address Developer ID Local IP address Cookie Engagement data

Appendix

Annex I to the 2021 Standard Contractual Clauses

This Annex forms part of the 2021 Standard Contractual Clauses and/or UK Standard Contractual Clauses, as applicable. By entering into the Standard Contractual Clauses incorporated in the Addendum, the parties also are agreeing to the terms of this Annex I. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Annex.

A, List of Parties

Data exporter. The data exporter is Customer and authorized affiliates of Customer, as described in the agreement. Contact: Customer's account owner email address, or to the email address(es) for which Customer elects to receive privacy communications.

Data importer. The data importer is Branch Metrics, Inc., 195 Page Mill Rd., Suite 101, Palo Alto, CA 94306, USA. Contact: Dominic Perella, Data Protection Officer, privacy@branch.io.

B. Description of the Transfer

Categories of Data subjects whose personal data is transferred. The personal data transferred concern the following categories of data subjects: End users of Customer's app(s) and/or websites into which the Branch SDK is integrated, and/or end users who click on Branch deep links.

Categories of personal data transferred. The personal data transferred concern the following categories of data: Personal data collected via Branch's SDK and Branch links, which includes the following types of device-related data: advertising identifier, IP address, developer ID, local IP address, cookie, engagement data.

Sensitive categories of data transferred. The personal data transferred concern the following special categories of data: None.

Frequency of the Transfer. Continuous basis

Nature of the Processing. The personal data transferred will be subject to the following basic processing activities: Processing necessary for the performance of the Branch Services, as well as related support and professional services as set forth in the Agreement, or where directed by other reasonable documented instructions provided by the data exporter.

Purpose of the data transfer and further processing. To provide the Services under the Agreement.

Anticipated duration of processing. For the term of any existing Order Forms between Branch and the data importer.

Transfers to subprocessors. The subject matter, nature, and duration of the processing is outlined at https://branch.io/third-party-list/.

C. Competent Supervisory Authority

The Irish Data Protection Authority will be the competent supervisory authority.

Annex II to the 2021 Standard Contractual Clauses

This Annex forms part of the 2021 Standard Contractual Clauses and/or UK Standard Contractual Clauses, as applicable. By entering into the Standard Contractual Clauses, the parties also are agreeing to incorporating this Annex II into the Agreement.

Description of the technical and organisational security measures implemented by the data importer in accordance with the UK Standard Contractual Clauses and the 2021 Standard Contractual Clauses):

Branch Information Security and Privacy Standards

Branch Metrics, Inc. is committed to adopt and adhere to the following technical and organizational security measures for software development, business operations and data privacy to provide a secure and safe platform service to our customers:

Governance

- Branch shall implement and maintain an Information Security Management System (ISMS) that meets or exceeds industry standards and that includes, without limitation, appropriate policies, governance structures, staffing, monitoring and assessment procedures.
- Security policies shall be approved by the Chief Operating Officer (COO) or the Information Security Management Committee (ISMC). Any exception must be authorized by the Head of Security or ISMC.
- Branch shall update security policies at least annually.

Workplace Security

- Branch shall install a visitor check-in system. All visitors must sign in at the front desk, and the visitor management application will notify the hosting employee to pick up the visitors. The visitor management application will issue a visitor badge. While visiting office premises, visitors must be accompanied by the hosting employee and wear their visitor badge in a publicly visible fashion at all times.
- Branch shall implement and maintain a secure mobile device management system to secure assets and information access for work. Company-issued devices and laptops are secured using a tested image and are protected using anti-virus and malware scanning software. To protect business data from data theft or exploit, external USB storage devices for laptops are prohibited (mitigated by mobile device management tool). Under Branch's BYOD (Bring Your Own Device) policy, personal mobile devices are required to access a separate guest wifi network if used in the office.

Physical Security

- Branch shall implement and maintain a program to ensure personnel physical access is revoked immediately upon termination or when access is no longer required.
- Employees must use an issued security access card to access office premises. Branch shall use physical locks inside the office building to secure network equipment and company assets. Access to server rooms should be restricted to authorized IT administrative staff. Security surveillance recordings are for review in case of any incident.

Organization Controls

- Branch shall implement and maintain policies and procedures, which shall be documented and approved by its senior management, to support the hiring, termination, code of conduct, ethics and background screening of all employees and contractors.
- Branch shall perform a background check using a reliable third-party service for each employee.
- Branch shall implement and maintain a security awareness program for employees, which provides basic IT security standards (during employee on-boarding), annual privacy and security awareness training, and individual personnel acknowledgment of intent to comply with corporate security policies.

Network Security Measures

Authentication and Password Policy Control

- Branch shall implement and maintain strong password management policies for all end user and system accounts related to the processing environment. Such procedures must follow recognized industry best practices in their configuration and management, including length and structure (commonly referred to as strong passwords).
- Branch shall implement a strong and complex password policy enforced for employees and developers. This should require at least 8 characters in length, including at least 1 uppercase character, 1 lowercase character, 1 number, and 1 special character. For employees, an industry-strength Mobile Device Management tool is used to enforce password policy in company-issued laptops. MFA (Multi-factor Authentication) is required to access Branch Metrics dashboard and applications.
- Branch shall implement an account lockout policy when users exceed the threshold of invalid login attempts.

System and Data Access

- Branch shall implement and maintain a secure system access mechanism and a remote access mechanism. Only authorized production support members and customer data administrators can access Branch's production systems backend and customer data on an as-needed basis via secured channels using virtual private network (VPN), jump boxes, secure shell (SSH) and multi-factor authentication (MFA).
- Branch's Web services require the use of service accounts and secure API tokens.

Logical Data Access

- Branch shall implement and maintain a logical system access provisioning process that meets or exceeds industry standards for all systems that access, process or store customer data and confidential information.
- Branch shall implement role-based security access.
- Branch shall implement and maintain a periodic logical access control review.

Operations Security Measures

Secure Software Development Lifecycle Process

- Branch shall implement a secure software development lifecycle process using agile development methodology, and periodically review security issues identified from static code analysis (SAST), Web application vulnerability scanning (DAST), penetration testing, and container security vulnerability scanning automated in the build pipeline.
- Branch shall engage third party professional security firms to perform network and application penetration testing in production environments annually. In addition, Branch will use security researchers from crowd-sourcing communities to identify exploits and security vulnerabilities.

Risk Management

- Branch shall implement and maintain a vendor and technology risk assessment strategy and risk mitigation methodology. The due diligence process will ensure systems security and data privacy details are reviewed, and security risks are mitigated before adoption.

Backup and Restore

- Branch shall implement and maintain data backup and restore processes to secure business data. Daily backups (snapshots) of data are made and stored in redundant locations. Only authorized personnel may access or restore any data from the backup datasets.

Security Monitoring and Logging

- Branch shall implement comprehensive system monitoring for Branch's cloud applications and microservices.
- Branch shall implement vulnerability and network intrusion detection controls. These controls will generate proactive alerts to notify the platform infrastructure team about any system events and suspicious activities

that may be potential security incidents. Detailed logging and audit reports are available upon request for security incident diagnosis and forensics.
- Branch shall implement and maintain security information and event management (SIEM) system. All system logs are redirected to a central infrastructure for event tracking, diagnosis and audit trail. In addition, with the use of SIEM, security team members can continuously monitor for any possible suspicious application behavior and unusual system events and respond timely to active and emerging security threats.

Security Incident Response Process

- Branch shall implement and maintain a security incident response program. The security incident response program shall define steps to be coordinated with the cross-functional incident response team in order to mitigate security incidents in a timely manner. All verified security incidents will be reported to the security incident response team in a timely manner. Depending on the levels of response, and pursuant to the applicable customer agreement, customers will be notified timely about the status and the remediation.
- Branch shall test the security incident response process annually.

Business Continuity

- Branch shall implement and maintain a business continuity program that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions ("Business Continuity Program").
- Branch shall conduct a business continuity test every twelve (12) months, including a review of the Business Continuity Program, roles and responsibilities, business documentation requirements, recovery strategies, Mean Time to Recovery (MTTR), Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), testing strategy and frequency.
- Branch shall implement and maintain a disaster recovery program that meets or exceeds industry standards and that provides a formal framework and methodology, including without limitation, a business impact analysis and risk assessment process to identify and prioritize critical business functions.

Change Management

- Branch shall implement and manage a change management system for planned and emergency software changes. There will be a workflow approval process in place to ensure change requests are prioritized and assigned.
- Branch shall implement a security patch management program. Software and security updates are pushed out periodically and on-demand. Critical security updates will be applied in a timely manner to mitigate any immediate security risks.
- Branch shall implement and manage a configuration management system. Configuration of systems and services is performed automatically by programs vetted for security deficits.

Data Security and Privacy Measures

Data Encryption and Integrity

- Branch shall provide industry standard encryption of customer data and confidential information in transit over public or leased circuits.
- Branch shall provide industry standard encryption of customer data and confidential information at rest on local laptops, mobile devices, shared drives, as well as on backend data stores.
- Branch shall implement and maintain logical data segregation that meets or exceeds industry standards to ensure customer data and confidential information is not viewable by unauthorized users.
- Branch shall implement input and output validation for data protection in the dashboard application. Business data is validated and checked for integrity in the backend microservices and in the API Web services. A data loss prevention tool shall be deployed in Branch's backend storage infrastructure to ensure data integrity.

Data Management and Protection

- Branch has implemented different data protection controls to ensure data privacy of customer data in accordance with applicable law. This includes protecting data at rest (data encryption), data in transit (secure data transport) and role-based system access control. Data access is restricted to authorized personnel, and production backend systems can be only accessible using MFA, VPN and company-issued laptops.
- Branch shall have the necessary processes and procedures in place to execute Data Subject Requests regarding personal data in accordance with applicable law in order to meet applicable legal requirements.
- Branch shall follow industry security best practices (e.g. Amazon, NIST) to destroy storage media, including cloud storage and also laptop hard drive before disposal.

Data Privacy

- Branch maintains a documented data privacy statement that describes what data Branch collects, how it is used and how it is shared available at https://branch.io/privacy.