

## FAQ: Onbe Contracts

This document aims to answer frequently asked questions our clients (“Client” or “you”) may have about Onbe, Inc. (“Onbe” or “we”) and our services to facilitate review of the Master Reseller Agreement (“MRA”). We know counsel and contracts professionals may be sent contracts to review without an accompanying full description of what Onbe does and why contracting for program management services may be unique, so below we have outlined common questions received to give helpful background. This FAQ document does not form part of the agreement between you and Onbe.

### 1. WHO IS ONBE AND WHAT DO WE DO?

Onbe is a corporate payouts gateway that manages and modernizes consumer and workforce payments for enterprise merchants and brands. Our payouts gateway enables clients to outsource their entire B2Individual disbursement operations, delivering a variety of payment choices from physical cards to instant digital options.

### 2. WHAT IS THE STRUCTURE OF ONBE’S AGREEMENTS?

- Master Services Agreement: contains typical legal provisions designed to govern the relationship between us and you. These terms apply to all programs.
  - Exhibit A – Provisions for Purchaser Agreement. Any of your entity customers (or your customer’s entity customers, if applicable, each being a “Purchaser”) that procure payment modalities or program management services must execute an agreement flowing down certain of the provisions from the Master Reseller Agreement.
- Program Agreement: sets forth the business terms for each program and contains brief product descriptions. All pricing and program-specific information will be in the Program Agreements. This document is comparable to a Statement of Work.

### 3. ONBE AS AGENT OF ISSUING BANK

To facilitate payments, Onbe is an authorized agent and program manager of certain issuing banks (the “Issuing Bank”). Onbe is not a licensed money transmitter or money service business. Onbe’s clients send funds to the Issuing Bank, which then issues payments. The Issuing Bank is not Onbe’s subcontractor. Rather, the Issuing Bank has obligations to oversee Onbe as an authorized program manager.

Each payment modality is the sole property of the Issuing Bank. The Issuing Bank will fulfill any obligation imposed on it by this Agreement pursuant to the Company’s agency relationship with the Issuing Bank. However, the Issuing Bank is not obligated to issue a Payment and may suspend or cancel any Payment or otherwise stop a Payment for reasons of compliance with Applicable Law, Rules or safe and sound banking practices.

### 4. PARTNERSHIP WITH OUR CLIENTS

We provide program management services to facilitate payments for your recipients. To this end, you will be responsible for providing accurate information, including funding amounts, payment recipient information, description of the payment use case, identifying information, and any other information as required by applicable law/regulation, including Know Your Business / Know Your Customer requirements. Onbe partners with clients to create a successful payment program and positive payment experience for recipients.

### 5. CAN CLIENT AFFILIATES LEVERAGE THE MRA?

Yes. Pursuant to Section 14 of the MRA, as long as Onbe obtains the appropriate “know your business” (KYB) information for the relevant affiliate, your affiliates can send funds for programs under the terms of the MRA. The affiliate must execute a Program Agreement which will specify that the affiliate is subject to the terms of the MRA and is responsible for its own obligations under the MRA and Program Agreement.

### 6. WHAT IS ONBE’S APPROACH TO DATA PROTECTION?

- Data Received. Onbe will receive data related to payment recipients. The type of data depends on the program, but we typically receive name, address and email address of payment recipients.



- PCI DSS. Onbe is certified in Payment Card Industry Data Security Standards (“PCI DSS”). This is the industry standard accepted set of information security policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of personal information.
- Protection of Cardholder Information. Onbe complies with the privacy provisions of all applicable law, including the Gramm Leach Bliley Act and Regulation P. Onbe maintains a comprehensive information security program which contains appropriate measures designed to ensure the security and confidentiality of data, protect against the unauthorized access to or use of such information and guarantee proper disposal of such information.
- Payment Data. Any information about a payment recipient that Onbe or the Issuing Bank maintains for the issuance and operation of payments is considered “Payment Data”. This Payment Data is owned by the Issuing Bank. Even though pieces of the Payment Data may have been provided by you, once that information is combined with a card number (PAN) and CVV or maintained for issuance of payments, it becomes Payment Data owned by the Issuing Bank (e.g. Onbe is no longer the Client’s processor of such information).
- GLBA and CCPA. Personal information subject to the Gramm-Leach-Bliley Act is exempt from California Privacy Laws according to Cal. Civ. Code §1798.145(e). In Onbe’s capacity as an agent of the Issuing Bank, any information you provide to Onbe is subject to the Gramm-Leach-Bliley Act.
- Information Security and Data Security Standards.
  - Onbe’s data protection technologies and controls follow PCI DSS standards. These include the use of strong passwords with multifactor authentication (MFA), access controls, encryption, firewalls, scheduled software updates, and endpoint protection solutions.
  - Onbe employees undergo mandatory recurring training on security best practices, including policies and procedures for accessing and sharing client data.
  - Onbe utilizes industry standard encryption algorithms and protocols to secure data communication and storage.
  - Onbe works with third party security service providers to conduct annual security penetration tests. Additionally, vulnerability scanning is conducted weekly and known vulnerabilities are mitigated in a timely manner.
- Privacy Program. The Onbe privacy program ensures proper use and disclosure of personal information, as well as fosters a culture that values privacy through awareness. The privacy program oversees regulatory change management, data subject requests (DSRs), and privacy impact assessments (PIA/DPIA); maintains policies and procedures; and conducts employee training and raises employee awareness.

## 7. DOES ONBE COLLECT PERSONAL HEALTH INFORMATION? DOES HIPAA APPLY?

No. Onbe does not collect PHI. In any case, Onbe, acting as an agent of the issuing bank, is exempt from HIPAA. HIPAA rules do not apply to banking and financial institutions with respect to payment processing activities pursuant to Section 1179 of HIPAA, which creates an exemption from compliance with HIPAA and accompanying rules when a financial institution is engaged in authorizing, processing, clearing, settling, billing, transferring, or collecting payments for healthcare.

## 8. SUBCONTRACTORS

Our superior vendor management program means Onbe and its clients can confidently rely on our subcontractors. We carefully select third party subcontractors through a rigorous due diligence process at onboarding, including information security reviews, with annual due diligence reviews conducted thereafter. We also spend thoughtful time and attention reviewing and negotiating all of our subcontractor agreements. We cannot grant our clients approval rights over subcontractors nor can we agree to “flow down” any contractual provisions to our subcontractors. Note Onbe’s subcontractors may include one or more of its affiliated entities, North Lane Technologies, Inc. and Swift Prepaid Solutions, Inc. dba daVinci Payments.