On-Demand Pay: The 4 Models and How They Work.

### Security and Compliance: Critical Evaluation Criteria

Evaluating on-demand pay providers securely and compliance capabilities deserves more attention than has been put on by our company at all. If done with exceptional diligence. Your IT and legal teams should be sure to dig into the following areas before agreeing to partner with any particular on-demand pay vendor.

#### Data Encryption

Data encryption should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest. The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

#### Access Control

Access controls should be placed on all critical systems and data, including segregated access to systems based on user role and system function. Users should have access to specific systems and data only as required for their job function.

#### Network Security

Network security should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest. The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

#### Personnel Management

Personnel management should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest. The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

#### Incentive-Based

Incentive-based programs should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest. The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

#### State Wage and Hour Laws

State wage and hour laws should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest. The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

---

**On-Demand Pay Scorecard.** To learn more about on-demand pay, see The On-Demand Pay Scorecard (link to overview page), of On-Demand Education Series (link to overview page), any HCM provider.

**On-Demand Pay RFP.** To learn more about on-demand pay, see The On-Demand Pay RFP (link to overview page), of On-Demand Education Series (link to overview page), any HCM provider.

**On-Demand Pay: The 4 Models.** To learn more about on-demand pay, see The On-Demand Pay: The 4 Models (link to overview page), of On-Demand Education Series (link to overview page), any HCM provider.

**On-Demand Pay: The 4 Models and How They Work.** To learn more about on-demand pay, see The On-Demand Pay: The 4 Models and How They Work. (link to overview page), of On-Demand Education Series (link to overview page), any HCM provider.

---

**Security and Compliance: Critical Evaluation Criteria**

- **Data Encryption**
  - Encryption in transit should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest.
  - The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

- **Access Control**
  - Access controls should be placed on all critical systems and data, including segregated access to systems based on user role and system function.
  - Users should have access to specific systems and data only as required for their job function.

- **Network Security**
  - Network security should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest.
  - The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

- **Personnel Management**
  - Personnel management should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest.
  - The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

- **Incentive-Based**
  - Incentive-based programs should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest.
  - The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.

- **State Wage and Hour Laws**
  - State wage and hour laws should include mandatory data encryption in transit. 256-bit AES, or other strong encryption methodologies such as AES 256-bit to secure client data while at rest.
  - The on-demand pay technology should include mandatory data encryption in transit (ex: SSL, SFTP) and strong encryption for cloud-hosting server communication, including multi-factor authentication and regularly updated passwords.