# **Fintech Infrastructure: Overview**



## **Leveraging APIs to develop a wave of new FinTech solutions**

Financial Technology (FinTech) is rapidly replacing in-person financial services with software and apps that provide banking, lending, payments, and investment management. The global financial crisis of 2008 led to distrust in legacy banks and opened the door to new consumer-facing FinTechs. This shift in consumer behavior has led to industry demand for FinTech infrastructure, a group of key integrations and application programming interfaces (APIs) that allow companies to build FinTech products and services. The Covid-19 pandemic further exacerbated FinTech adoption, as consumers shifted to digital and contactless financial services.

Building infrastructure in-house can be challenging as it may require integrations across multiple organizations that each offer a range of products and services that must be handled separately and on a case-by-case basis. For example, a single bank may offer savings accounts, lending services, mortgages, and credit cards with each product requiring its own technical infrastructure. Therefore, a growing number of FinTech companies are turning to FinTech infrastructure-as-a-service (IaaS) providers. IaaS providers build common infrastructure platforms for a dedicated purpose (such as banking, lending, payments, etc.) which can be used by multiple enterprises to build their respective FinTechs.

### 

### 

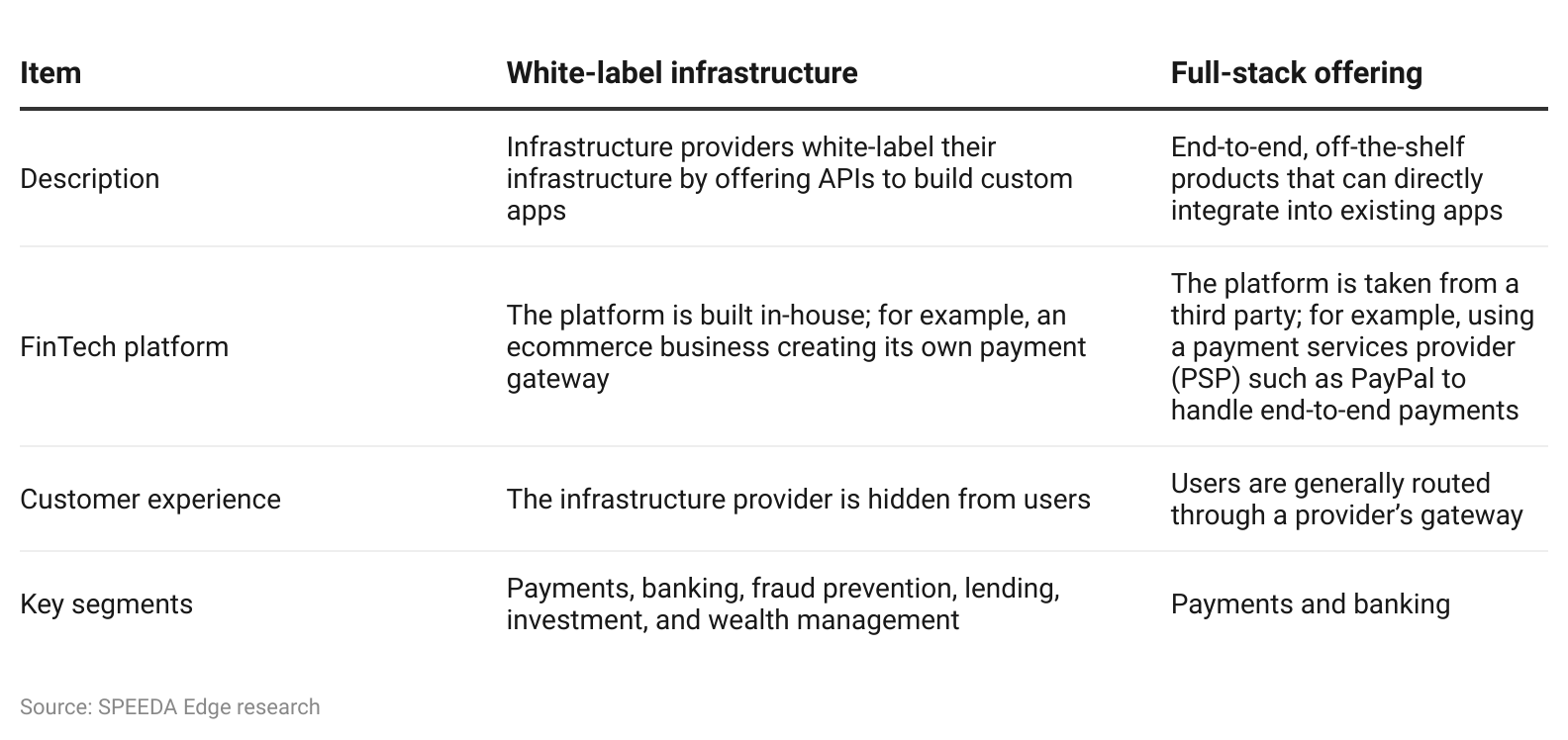
### **FinTech infrastructure providers create a common platform to access multiple integrations**

****

Source: SPEEDA Edge research

FinTech IaaS can be offered in two forms: 1) as white-label infrastructure, and 2) as a full-stack service.

### **White label and full-stack; the alternatives to in-house**



## 

## **FinTech infrastructure can embed financial services across industries**

FinTech infrastructure is best classified by the end-user therefore we have identified the following five main segments within the FinTech infrastructure provider industry based on the type of financial service embedded into a given FinTech.

### **FinTech infrastructure primarily comprises five segments**



FinTech infrastructure providers typically have a recurring revenue model, charging a subscription-based on factors such as transaction values, volumes, number of users, etc. These providers may also charge an implementation fee.

Although businesses across segments have the liberty to choose the most suitable model, we have identified the following as the most prevalent business models for the industry.

**Possible revenue models and corresponding industry segments**

# 

# **Driving Factors**

## **1. Enterprises developing new FinTechs and existing FinTechs expanding operations**

Infrastructure-as-a-service (IaaS) startups directly benefit from an increase in the number of firms building FinTechs—including a growing number of non-financial companies including retailers and technology platforms—from an increase in the usage of existing FinTechs.

* Investment deals in FinTechs in the Americas (including VC, PE, and M&A) have grown over the period 2020–2023 (up to 2,136 in 2023 from 1,997 in 2020), with the highest deal count of 3,633 recorded in 2021.
* The number of FinTech startups worldwide has more than doubled over the period 2020–2023, reaching over 26,000 in 2023 (with ~40% of US startups) from over 12,000 in 2020.

As of 2022, nearly 80% of Americans are reportedly using financial apps for payments, tax filing, online banking, investing, budgeting, and lending, among other use cases. Despite the widespread use, however, no single FinTech application has exceeded 70% market penetration according to [Plaid](https://sp-edge.com/companies/85350), indicating significant potential for future growth. Meanwhile, Grand View Research projects the US FinTech market to grow at a CAGR of 16.6% over the forecasted period of 2023–2028, as adoption continues to expand.

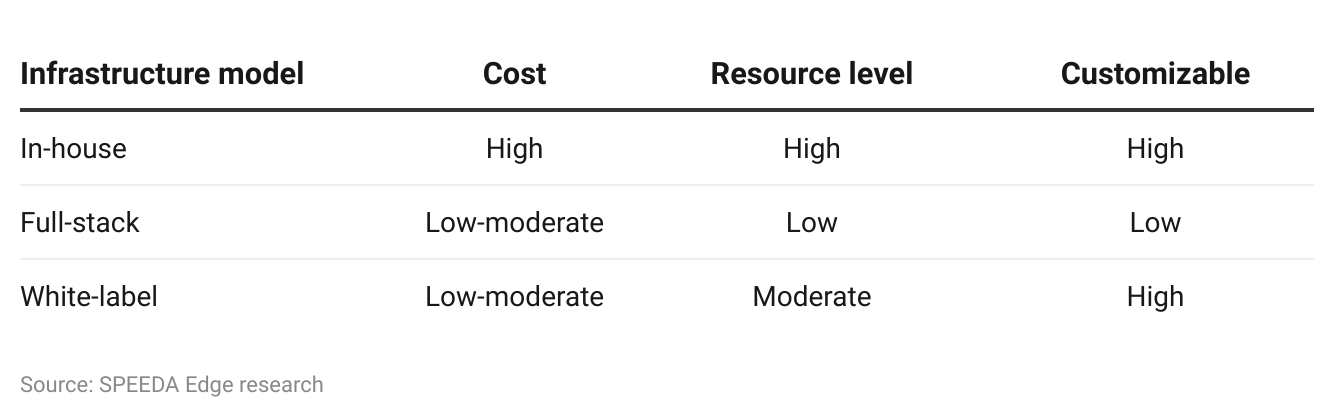
* Growing consumer adoption is attributable to FinTechs’ focus on previously untapped segments such as marginalized demographics and users with thin credit histories, while also winning on cost and convenience.
* Small and medium enterprises (SMEs) are adopting FinTechs to gain access to a wider range of features and the availability of service.

## **2. FinTech IaaS is more cost-effective for resource-constrained enterprises**

Using FinTech IaaS alleviates the need to build complex infrastructure in-house, and allows businesses to build their own FinTechs with fewer resources at a lower cost. While this primarily benefits the specialist FinTechs developing new solutions, it can also help legacy financial institutions (such as incumbent banks, credit unions, and community banks) to modernize their digital solutions. Studies in 2023 have indicated that as many as 88% of bank and credit union CIOs believe that integration challenges hamper digital transformation. This could be addressed through infrastructure platforms, which enable transformation using fewer resources.

Once a company decides to go down the IaaS route, it will need to decide between a full-stack or white-label infrastructure solution. Full-stack solutions require fewer resources, while white-label providers are highly customizable.

### **Comparison of FinTech infrastructure models**

**3. Regulatory compliance presents in-house development challenges**

FinTechs are required to comply with a range of domestic and international regulations from the front-end through infrastructure and to the client-side, presenting real and costly challenges to FinTech development.

Although infrastructure providers do not ensure front-end compliance with the front-end processes, these companies minimize the compliance burden relating to infrastructure issues such as banking licenses and payment APIs. For instance, FinTech infrastructure providers such as Volt and Enfuce secured electronic money institution (EMI) licenses from the UK's Financial Conduct Authority (FCA) in February 2024 to ensure regulatory compliance with offering electronic money services, card issuing, and payment processing services in the UK.

FinTech infrastructure companies often face the following common compliance challenges

* **Compliance with local regulatory bodies to enable cross-border transactions:** For instance, operating in Europe and the UK requires compliance with Europe’s Payments Services Directive (PSD2) and approval of a banking license by the FCA (Financial Conduct Authority). Griffin secured its banking license in March 2024 from the UK's financial services regulators, the Prudential Regulation Authority (PRA), and the FCA, allowing it to launch as a fully operational bank.
* **Scrutiny from multiple regulatory bodies:** US FinTech providers fall under the purview of several regulatory bodies with broad mandates including the SEC and FTC.
* **Fragmented regulatory landscape:** FinTech providers are also required to comply with state-level regulations in areas that lack clear federal statutes.

To overcome these obstacles, FinTechs typically partner with banks and other financial institutions to offer them a platform to provide their services such as loans, account maintenance, etc. However, this strategy can face higher costs, complexities, and regulations due to the burdens placed on banks as they are held accountable for their FinTech partner’s actions.

# **Risks to Growth**

## **1. Long sales cycles and development periods could stagnate growth**

FinTech infrastructure providers face long sales cycles because they typically build key systems for FinTechs such as core banking or payment systems, which change only about every five to ten years—especially among larger enterprises. Sales cycles are further impacted by the stringent and time-consuming procurement and onboarding process for new vendors at large enterprises.Product development may also take longer—up to 16 - 24 months—compared to consumer FinTechs due to regulations, and technical requirements demanded by enterprise customers.

## 

## **2. Rising vulnerability to hacking with sensitive data stored in the cloud**

FinTechs and IaaS providers tend to be more vulnerable to data breaches and denial-of-service (DOS) attacks than legacy financial services because they are digitally native and typically store customer data and financial information on the cloud. The impact of cyberattacks on infrastructure providers may also be larger than attacks on individual FinTechs as multiple FinTechs may share infrastructure and could therefore face downtime.Cybersecurity vulnerabilities, along with the lower awareness and trust in FinTechs among non-adopters, could slow FinTech adoption and therefore reduce demand for FinTech infrastructure as a whole.

## **3. Increased risk of compliance breaches with tightening privacy laws**

Privacy laws have been tightening across the globe with the adoption of the General Data Protection Regulation (GDPR) in the EU in 2016 and the California Consumer Privacy Act (CCPA) in the US in 2020. These laws substantially impact the FinTech industry, as FinTechs and infrastructure providers alike handle a range of personal information and finance records. For instance, In [August 2021](https://sp-edge.com/updates/4785), diversified FinTech infrastructure provider, [Plaid](https://sp-edge.com/companies/85350), agreed to pay USD 58 million (around 34% of its annualized revenue as of December 2020) in a class action lawsuit settlement, over claims the company used banking login credentials to share data with third-party firms without prior consent.

In addition to managing and connecting financial information, FinTechs also typically use AI and ML to comb through personal customer data such as online spending, social media patterns, and digital footprints to make financial decisions such as credit limits and risk profiles which can potentially lead to privacy breaches.

The use of biometric verification in FinTech applications, while enhancing security and improving user experience, also imposes increased risks of compliance breaches. For instance, [Veriff](https://sp-edge.com/companies/492317) settled a class action lawsuit for USD 4 million in [February 2023](https://sp-edge.com/updates/16805), for failing to comply with the Biometric Information Privacy Act (BIPA) in obtaining consent before collecting facial geometry scans for identity verification.

*Last updated: June 2024*

©2024 Uzabase, Inc. All Rights Reserved. The information contained herein: (1) is proprietary to Uzabase Inc. and/or its content providers; (2) may not be copied or distributed; and (3) is not warranted to be accurate, complete or timely. Neither Uzabase Inc. nor its content providers are responsible for any damages or losses arising from any use of this information.