Your Free Guide: How to perform FinTech Testing

Packed with practical guidance to ensure that you implement and deliver the right test approach, including automation, that will enable you to meet your business objectives and achieve the best ROI.
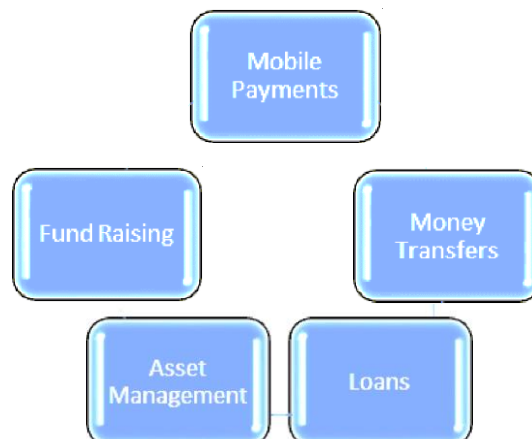
FinTech Testing

FinTech is short for Financial Technologies and is the term used to represent the digitalization of traditional financial services. FinTech technologies are undoubtedly going to disrupt and define how financial services operate in the future, for example they will shape how consumers interact with banks and how we pay for items online. Traditional financial organizations are going to have to adopt and embrace the FinTech revolution or risk getting left behind.

In recent years there has been a large increase in investment and level of interest in the FinTech market:

- PwCs insight in FinTech Report highlighted that more than 80% of traditional financial services are threatened by the FinTech revolution.

- Gartner predicts that by the end of 2019, 25% of retail banks will use startup FinTech providers to replace legacy online and mobile banking systems.

FinTech Services Can Be Separated into The Following Categories

FinTech Testing

The FinTech model creates several technical challenges for testing and QA. A typical FinTech start-up delivery approach is fast paced, agile and extremely customer focused. Quality Assurance must respond with a testing approach that enables the fast delivery with regular software releases and is still able to measure quality.

A testing approach must focus on continuous integration and automated regression, so as daily code drops are released then testing can ensure a good coverage of features without slowing down the delivery. A reliance on any manual testing must be kept to a minimum, with a focus on any key features or priority issues.

Automation Testing	Performance Testing	User Experience
Data Quality	Security	

As with any financial services company, security must be a high priority to ensure the company and customers details are protected. Finally, one of the main success factors of FinTech companies, compared to traditional financial organizations, is the focus on user experience. Testing must ensure UX is included in the process with a continual feedback loop into development, with UX testing considerations initiated from the start of any new project.

Automation Approach

FinTech delivery is lean and quick, with a focus on an agile / continuous integration development process. Operational efficiency is a necessity for any FinTech. An automation framework is essential to enable this transformation, helping to increase quality whilst in parallel reducing the amount of effort and spend on managing the testing. Also, to maximize the benefit of any automation strategy there must be a good working cooperation between development and test.

The following looks at some of the key areas to consider when automating integration with third-party payment gateways and the test scenarios.

1. Most of the common payment gateways provide a web-based integration which can be easily tested using Selenium and direct GUI less library.

2. First need to identify web elements using various locators.

3. Verify each call to third-party payment gateway contains unique id which can be used later to cross verify the transaction on both sides.

4. Write tests to verify both success and failure scenarios. Create mind map of positive and negative scenarios, then look how they can be translated into automate tests.

5. Payment gateways provide test data to verify various scenarios (e.g. invalid CVV, blocked card etc.).

6. Try to simulate internal failures and test how those are handled. e.g. payment gateway returned success, but transaction failed due to internal issue

7. Write tests to check no response scenarios and call back after that.

8. Verify the data stored in DB, it is encrypted. Review latest data privacy laws such as GDPR to ensure required standards are met.

9. Verify data passed to payment gateway is encrypted and transferred over https only.

10. Validate no sensitive information is passed to or received from payment gateway

11. Verify cross currency transactions to understand how the system processes different currencies and complications it may create.

Payment Processing Manual Test Scenarios

The next section outlines some of the manual test scenarios that should be considered when performing online payment processing testing:

1. Data should be transferred securely over https (not http).

2. Sensitive data (e.g. card number etc.) should always be transferred encrypted.

3. Sensitive data, if stored in DB, should be stored in encrypted form.

4. All the data should be transferred using session ids with auto expiry.

5. In case of parallel transactions, accounting in the main account should be synchronized and should not allow multiple transactions to update in parallel.

6. All transactions should maintain atomicity.

7. Transactions should be allowed based on the defined rules only.

8. In case of integration with third party payment gateways, all interactions should happen securely from only white-labelled IPs i.e. it should reject all requests coming from unknown (public) IPs.

9. If any third-party payment SDK is used, then all transactions should have a unique external id which should be different from internal id used within app.

10. There should be some ways to validate that the requests are coming from authentic users (by using user's device specific id etc.)

11. There should an auditing system to alert in case of fraudulent/suspicious activities and to resolve any issues faced by users.

12. Data should never be deleted. It should be archived if required

13. System should be capable to handling many concurrent user sessions and requests

14. There should be at least one backup server to process requests if main server fails.

15. Access to database should be highly secure and should be allowed from white labelled IPs only.

FinTech Test Summary

FinTech companies are revolutionizing how financial services are delivered with a focus on fast paced agile delivery and user experience. QA will need to focus on the following key areas to ensure it continues to add value to the process:

- [Security](#) — don't wait to come under attack, build in application security from the start.

- [Data Quality](#) - ensure data is correct / secure / and compliant to the latest regulations.

- [Continuous Integration](#) — implement the right automation framework to meet your objectives.

- [UX (User Experience) Testing](#) — provide first class UX experience.

- [Performance](#) — ensure your platform / services continue to work at peak times.

Tessolve are helping FinTech organizations around the world deliver products and services that are reliable, safe, and secure. Our consultants are trained to increase the effectiveness, efficiency, and coverage of your software testing. Establishing our automation Centre-Of-Excellence has enabled Tessolve to build a wealth of automation expertise and experience. Tessolve will ensure you implement and deliver the right test approach to enable you to meet your objectives and business demands, plus ensure your ROI is achieved.

Discover How Tessolve Can Help with your Fintech Testing

www.tessolve.com