



EVALUATION GUIDE

Disclaimers

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Instnt products described herein. You agree to grant Instnt a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Instnt disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice.

Instnt, the Instnt logo, are trademarks of Instnt or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Table of Contents

Introduction	4
Welcome to Instnt.....	4
How We Work With You.....	5
Enabling Your Growth Strategy	6
Why Instnt	6
Instnt ROI Model	8
Instnt Use-Case Examples.....	9
How Instnt Works	10
Testing Instnt	13
Instnt Solution Architecture.....	17
Instnt Pricing and Liability Model.....	Error! Bookmark not defined.

Introduction

Welcome to Instnt

Thank you for considering Instnt for your customer onboarding solution. We take great pride in helping businesses sign up more good customers. We aim to deliver frictionless and fraudless experiences that drive rapid top line revenue growth and a reduction in bottom line costs for our customers. We are driven by the performance and value we can deliver to you and your customers. Instnt contractually guarantees its performance! If we can't help you sign up more good customers, reduce your false positive rate, reduce your costs, and reduce your fraud its possible we are not the company for you.

We created Instnt because we believe the prevailing approaches to customer onboarding and new account fraud are fundamentally broken and a paradigm shift is needed. A new disruptive vision, an orthogonal approach to the status quo is required to reduce the massive waste and legacy solutions. How are billions being spent on fraud protection and the industry is still losing 20-40% of good customers and over 26% of potential revenue? Fear and risk of fraud losses force companies to implement draconian risk management controls that create dreadful customer experiences and unnecessary friction. Online businesses put delivering frictionless customer experience as a top priority, but existing fraud prevention programs are blocking up to 40% of good users.¹ Then why do companies focus on fraud vs. the top line growth that is being inhibited?

Three overarching and codependent industry practices are being employed to manage the balance between signing up more good customers and avoid signing up bad actors that commit fraud. As you work with Instnt to build your business case for using the Instnt AI powered Customer Onboarding Platform, we will help you address these challenges and reveal a business model and a simple approach to signing up more good customers and growing your top line.

1. **Point solution orchestration:** Stop orchestrating around multiple technologies to de-risk customers. The assumption that assembling more IT services to access more data to re-risk users is fundamentally flawed. This is what we do best as a highly scalable performance based on demand service.
2. **Risk reward management:** It is all too common to employ risk reward management practices predicated on turning away good customers to avoid signing up bad ones. This is an outdated practice resulting in false positive rates as high as 46%. At Instnt, we guarantee we will reduce your false positive rate by 50%. We manage the risk and you receive the reward in the form of more good customers.
3. **Business model conflict:** When your company takes all the risk for the services you have procured and deployed; this is business model conflict. At Instnt, we believe in getting paid for performance, that also means we take the losses off your books. We provide three indemnification schedules: \$1 million, \$10 million and \$100 million in third party, synthetic ID and certain types of chargeback fraud.



Let us help you do what you do best, by helping you sign up more good customers with a business model that works for you.

Thank you for considering Instnt
Sunil Madhu CEO, Mimi Salcedo CPO

¹ Why 40% of consumers abandon banking applications; © Signicat 2018

How We Work With You

Evaluating Instnt will be a collaborative process designed to help you and your colleagues assess, test and ensure Instnt services are a good fit for your company. This evaluation guide provides the framework for building your Instnt business case, provides an introduction to the Instnt platform features and functions, outlines the Instnt assurance and indemnification coverage and provides the criteria and approach for testing and using Instnt to onboard your customers.

The Instnt alignment map in figure 1, is value driven and designed to ensure the right people are involved in the decision-making process at the right time. We advocate including leadership from your Product and Marketing, Treasury (Finance, Risk, and Compliance), IT and Operations, and Legal teams. Your company will be assigned a Community Growth Manager responsible for stewarding you through the decision-making process and aligning with Instnt Product, Engineering, Operations and Legal resources. The Community Growth Manager will be your relationship manager responsible for capturing the necessary ROI data, testing key performance indicators, processing legal documents and establishing performance pricing.

When you are ready to test Instnt a Customer Success Manager will be assigned to your account. The Customer Success Manager will work with your product and IT resources to ensure effective integration, monitoring and reporting of the 60-day Instnt testing. If Instnt successfully meet the false positive rate reduction, fraud reduction and operational key performance metrics the Customer Success Manager will support the migration to full-service integration and delivery.

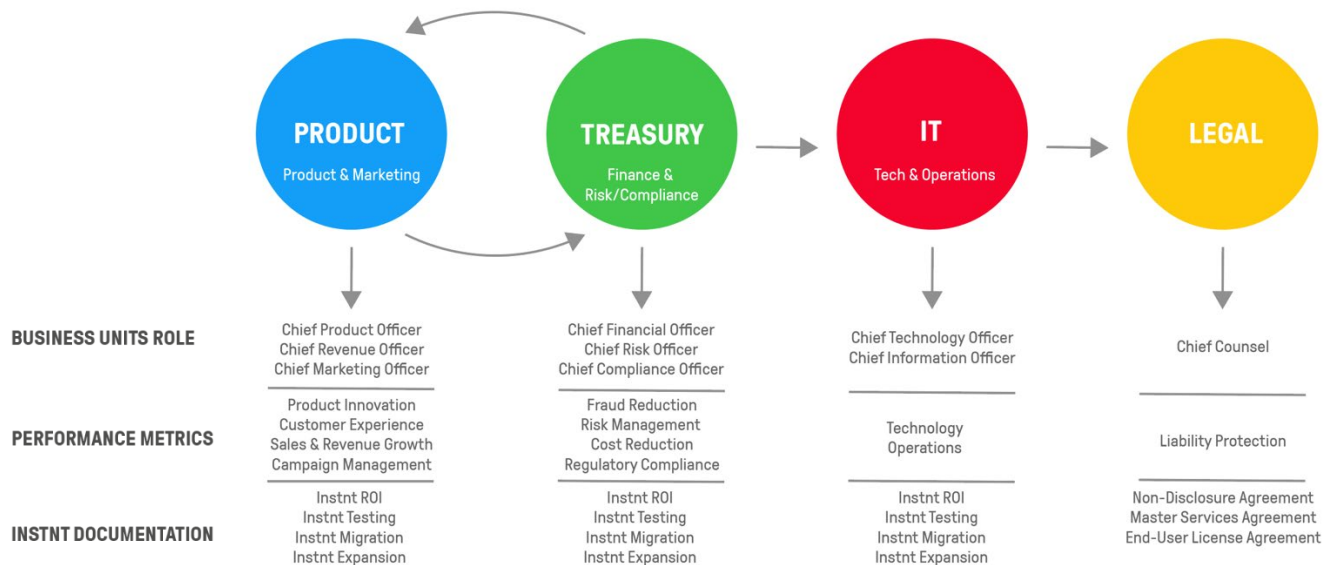


Figure 1. Alignment Map

The evaluation process can be completed in as few as two weeks and can run in parallel to the testing of the Instnt services which will take 60 days. Each of the respective business units involved in the evaluation of Instnt are required to provide relevant ROI, testing, and migration information to ensure we can maximize the value of our service.

Enabling Your Growth Strategy

Why Instnt

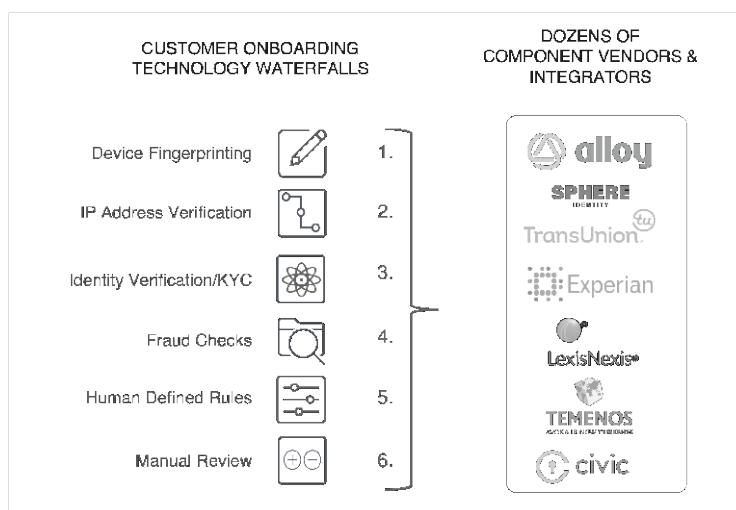
At Instnt we want to enable your rapid growth. We will do this by helping you sign up more good customers with a flexible drag and drop dashboard and a service that can be operational in a matter of hours. As simple as Instnt is to deploy and use your company is still required to create the business rationale for migrating to Instnt's AI-powered customer onboarding platform.

We provide an ROI framework for developing the business case and your Instnt Community Growth Manager will work with your team to determine and capture the metrics for potential revenue growth, fraud reduction, capital and operational expense reduction and for long term strategic growth leveraging Instnt's #singlesignup.

Assessing Instnt also requires reviewing delivery and operational capabilities, the risk management model and the cost of the services we offer. Three overarching and codependent industry practices are being employed to balance signing up more good customers and avoid signing up bad actors that commit fraud: Point solution orchestration, risk reward management practices and business model conflict.

1. Point Solution Orchestration

Point solution orchestration involves the programming and integration of third-party information and tools required to de-risk a user, assert a scored high level of validation that the person on the other end of the transaction is a real and good customer engaged in signing up for your product or service. Companies employ waterfall risk models, applying the cheapest and simplest tools at the top of the stack. The further down the funnel they get the more expensive and complex the solutions become. The assumption being that the more tools you hook into, the more information you have, should give you the ability to reduce the risks of various types of fraud. This is a flawed assumption.



Companies attempt to verify against many forms of identity verification, behavioral analysis, IP verification, device tagging, fraud checks, document verification, AML, watchlist screening, and employing human-defined rules. Some companies orchestrate around solutions like Alloy and IDology or build their own home-grown orchestration engines, building analytical layers on top suites of different tools creating new account fraud detection stacks. The challenge is that these technology waterfalls produce significant false positives. You continue to lose good customers as a consequence of the friction caused by the non-performance of these waterfalls. Moreover, human defined orchestration rules need constant upkeep in a reactive rather than proactive manner, compared to modern machine learning approaches.

When the engine doesn't scale, companies tighten the screws on how many new customers they accept and employ large teams of people to catch the customers that fall out of the process, resulting in manual reviews. This is ultimately vendor roulette and literally a gamble. The vicious cycle of fraud growth and the desire for better business results support a cottage industry of hundreds of vendors. Making it harder for your company to know what to use and how to effectively scale your customer onboarding services. IT, risk and compliance are often treated as cost centers and are naturally fighting for budget. Underfunded teams struggle to get the expertise to get it right more than 95% of the time, making it mathematically and financially unviable to balance growth and fraud loss expectations.

Legacy systems also often restrict customer onboarding workflows, building needless friction into the customer experience, forcing the user to input too much information at once, consequently raising the abandonment rate. Legacy customer onboarding services also make it difficult for product, marketing and sales teams to rapidly test new customer onboarding workflows or to be flexible in supporting different workflows for different customer types.

Instnt's Answer for Point Solution Orchestration

Stop orchestrating around an outdated technology stack. The Instnt AI-powered customer onboarding service provides the entire technology stack a company needs to sign up more good customers and reduce fraud. Instnt services include identity verification, behavioral analysis, IP verification, device tagging, fraud checks, document verification, AML, watchlist screening, and cohort analysis based on machine learning. Instnt offers a drag and drop dashboard to design as many branded forms, workflows and capture as much information as is necessary, as a service, and can be implemented in a few hours.

2. Risk Reward Management Practices

Every company employs risk reward management practices to balance the number of good customers being signed up to avoid the number of bad actors that can commit fraud. Combatting fraud is a tradeoff between the amount of risk you should assume correlated to the amount of revenue you can generate through your digital channels. However, when your top line growth is inhibited due to your risk management practices, and if the focus on fraud is outweighing your ability to sign up more good customers, perhaps the risk management pendulum has moved too far in the wrong direction away from revenue growth. Although fraud is a part of the business of signing up new customers, it shouldn't be costing you 20% to 40% of your good customers or 26% of your potential revenue to fight it.

The scale, complexity and variety of fraud companies are exposed to force tighter risk management governance and a focus on silo operations to combat the problem. In 2013 Gartner published the "Security and Risk Management Scenario Planning - 2020" in which they predicted the risk-based governance models being employed could limit a company's top line growth. Four scenarios were identified to address the distributed highly scalable organized crime scenarios we actually operate within today. The two scenarios that are of interest to Instnt and your company are Regulated Risk and Coalition Rule.

We are operating in the regulated risk scenario today whereby regulators simply have not and cannot keep up with data use and business model innovations being developed around personal information, resulting in de facto standards that are slow to develop. There is no denying we need regulations and compliance, however for the most part, regulations are a reaction to the external environment vs. a proactive approach to resolving the types of sophisticated risk we are witnessing, effectively making them a checkbox.

According to the same Gartner report, the scenario that best resembles today's environment and actually has the potential for the most risk-reward value is the coalition rule model, in which a coalition of companies and their collective intelligence is the best way to combat the rise of fraud and cybercrime. The lack of a coalition model focused on the collective health of our digital ecosystem is limiting your generative growth, the creation of new sources of value vs. the primary focus on just keeping the bad guys out.

Instnt's Answer to Risk Reward Management Practices

Instnt is founded on a coalition model and we are building the community of companies whereby the collective intelligence is used to combat the fraud, reduce waste and improve performance. We contractually guarantee we will reduce your false positive rate by 50%. We manage the risk and your company receives the rewards in the form of more good customers.

3. Business Model Conflict

At Instnt we believe there we can eliminate two business model practices to deliver value back to our customers.

1. Business model conflict occurs when your company takes all of the liability for the services procured. When you pursue an independent orchestration approach you pay transactional pricing and cannot receive liability assurances from the vendors supporting your technology stack. Vendors explicitly call out the lack of liability indemnification because you own the custom integration of the services, risk controls and fraud loss decision making.
2. Business model conflict also exists with the transactional use of personal identifiable information by credit bureaus and other static data providers. These vendors are essentially monetizing consumer data that has already been hacked multiple times, using the same user demographic information to support the technology orchestration model explained earlier. The risk of using static, dated information from credit bureaus and static data providers who are the very breeding grounds for synthetic ID fraud is flawed. The demographic of Millennials and Generation Z customers that are driving the economy for the next 40 years are all considered 'thin-file' by these bureaus, suggesting there isn't sufficient information about them in the on-demand economy they have spurred. When your company takes all the risk for the services you have deployed, this is business model conflict.

Instnt's Answer to Business Model Conflict

Instnt's services are priced on a performance basis, we get paid for helping you sign up more good customers and we contractually take the fraud losses of your books. We provide three indemnification schedules: \$1 million, \$10 million and \$100 million in third party, synthetic ID and certain types of chargeback fraud. Instnt stands behind its services for up to \$100 million per customer by arbitraging the fraud using our own AI engine.

Instnt customer verification services do not rely on static data or outdated information from the credit bureau services. Instnt is built on a proprietary suite of services that also help companies' identity and verify thin file customers.

Instnt ROI Model

	Product Annual lifetime Value	New Customer Accounts Per Month	New Customer Accounts Per Year	False Positive Rate	True Positive Rate	Annual Capital and Operating Expenses	Fraud Losses	Other KPI Growth Goals	Summary
Current, Planned									
With Instnt									
Total Savings									

Instnt Use-Case Examples

Regardless if you are a fledgling start-up, a challenger bank or a fortune 100 company, the Instnt AI powered customer onboarding platform can be used to drive value across a wide variety of vertical industry use cases including the following:

1. Financial Services
 - a. Debit account opening
 - b. Virtual debit, credit account linking
 - c. Credit and Loan instrument application
2. Insurance applications
 - a. Health savings plan account opening
 - b. Brokerage account opening
3. eCommerce
 - a. Account opening
 - b. Credit card applications
 - c. Product purchase and leasing
4. Healthcare
 - a. Account opening
 - b. Insurance claims

How Instnt Works

The Instnt AI-powered customer onboarding platform is offered as a fully managed multi-tenant service. Figure 2 provides a graphical representation of the underlying services included.

The platform is accessed through an intuitive web-based dashboard illustrated in Figure 3, where administrator level access allows for the provisioning of additional users who can build branded forms, develop multi-step workflows and establish the business rules for where to send the data for good customers, bad actors and customers that may need additional review.

The core services include geolocation, network analysis, user behavior analysis, device intelligence, predictive analytics and machine learning. The sign-up form build process also allows for the optional selection of Identity and Document Verification as well as KYC.

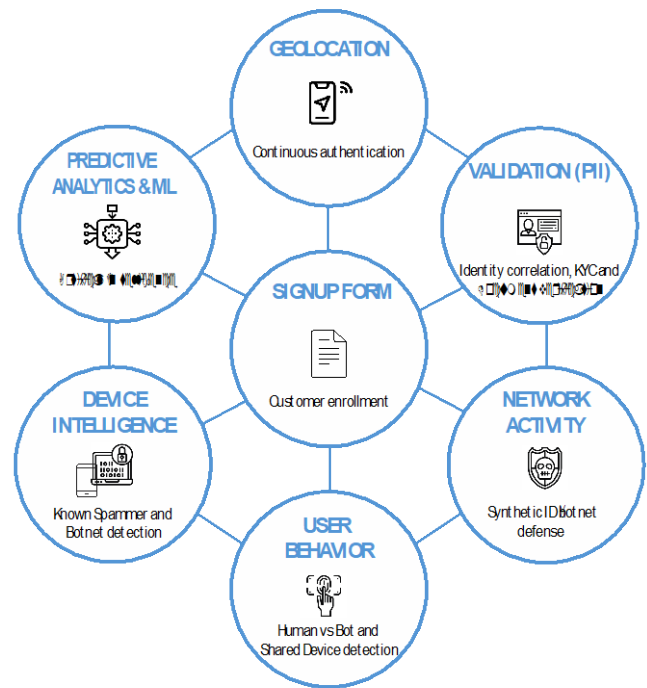


Figure 2. Instnt Services

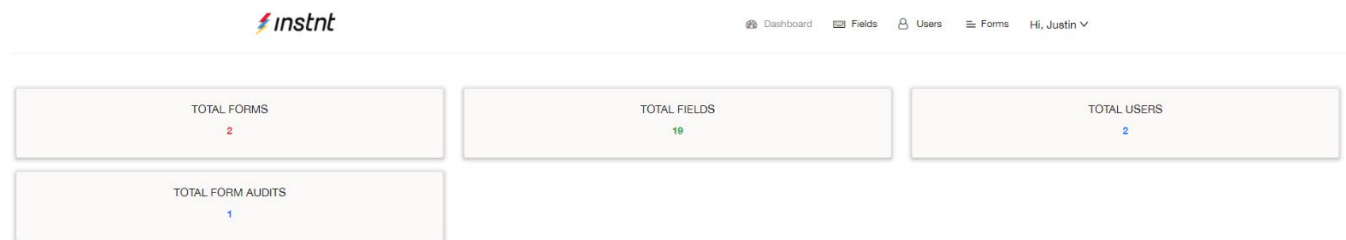



Figure 3. Instnt's Dashboard

The first step when creating an Instnt powered form is the Overview Page, which contains the following entry fields:

- **Form Name:** The form's internal name, viewable on the Forms page;
- **Start Form Template Dropdown:** Instnt offers a variety of form templates to choose from based on common form types in order to streamline the form creation process;
- **Type of Form:** Instnt form creation tool allows for the creation of both single step and multi-step form formats.

Once the relevant information has been entered into the entry fields on the Overview page, the user is able to proceed to second step in the process and build branded forms.



My Forms
Add Form
Hi, Justin

Sign-up Form
Overview
Builder
Business Rules
Confirmation
Cancel

Get Started

Create a name for your form so you can easily reference it later, then choose its basic settings.

Form Name*

Start From Template?

No

Type Of Form

Single-step

Multi-step

[Save For Later](#)
[Next](#)

The Form Builder page contains a rich feature set of choices to design your forms, including a drag and drop field placement column, the ability to add formatted columns, a preview pane for the form itself, and an editable CSS code block for advanced users.

dsdsdd
Overview
Builder
Business Rules
Confirmation
Cancel

Form Preview

Refresh

Title

Sub title

Drop field here

Submit

Powered by instnt

Build Your Form

The "Form Preview" is everything your customers will see. Configure a title, subtitle and button label then select which fields you'd like to add to your form.

Form Details

Form Title*

Form Subtitle*

Submit Button Label*

Add Columns

Add row with one column
Add row with two column
Add row with three column

Add Form Fields

☐ Email Address
☐ First Name
☐ Surname
☐ Country
☐ Street Address
☐ City
☐ State
☐ Zip Code
☐ Mobile Number
☐ Social Security No
☐ Company Name
☐ Username
☐ Date of Birth
☐ Order Amount
☐ Account Creation Date
☐ Submission Date
☐ Previous Order Count
☐ LastOrder Date
☐ I accept terms and condition

CSS

```

1  #v584326100000 {
2    background: white;padding:10px;
3  }

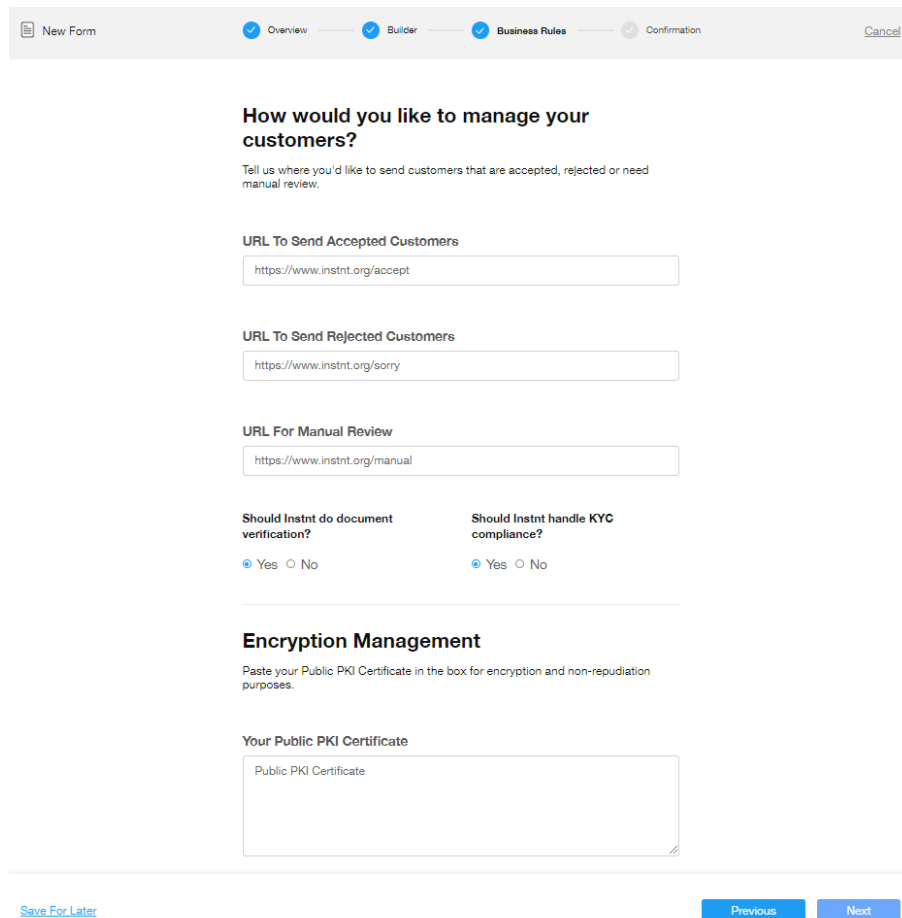
```

[Save For Later](#)
[Previous](#)
[Next](#)

The third step when creating an Instnt-powered form is the Business Rules page that contains the following entry fields:

- URL to Send Accepted Customers: If Instnt's API believes that a customer has passed a fraud detection check, that customer will be sent to the URL listed in this field;
- URL to Send Rejected Customers: If Instnt's API believes that a customer has failed a fraud detection check, that customer will be sent to the URL listed in this field;
- URL for Manual Review: If a manual review is required, enter a relevant URL for that process here.

Beyond these entry fields, Instnt also provides the option to have documents independently verified by the company as well as allow Instnt to handle KYC compliance. For either option, the user can select the yes/no radial buttons to enable/disable them.



The screenshot shows the 'Business Rules' configuration page in the Instnt interface. At the top, a progress bar indicates the steps: Overview, Builder, Business Rules (current), and Confirmation. A 'Cancel' link is on the right. The main heading is 'How would you like to manage your customers?'. Below it, a subtext says 'Tell us where you'd like to send customers that are accepted, rejected or need manual review.' There are three text input fields: 'URL To Send Accepted Customers' (with 'https://www.instnt.org/accept'), 'URL To Send Rejected Customers' (with 'https://www.instnt.org/sorry'), and 'URL For Manual Review' (with 'https://www.instnt.org/manual'). Below these are two sets of radio buttons: 'Should Instnt do document verification?' and 'Should Instnt handle KYC compliance?', both with 'Yes' selected. The bottom section is 'Encryption Management', with subtext 'Paste your Public PKI Certificate in the box for encryption and non-repudiation purposes.' It features a large text area labeled 'Your Public PKI Certificate' with the placeholder 'Public PKI Certificate'. At the bottom, there is a 'Save For Later' link, a 'Previous' button, and a 'Next' button.

Instnt also allows for the addition of Public Key Infrastructure (PKI) Certificates to manage encryption and non-repudiation.

Once the PKI Certificates have been added to the Encryption Management pane, the user is able to finalize the form and generate the source code for the fourth and final step of the process, creating the Confirmation page. The Confirmation page contains the source code for your sign-up form in both Div and iFrame and includes a dropdown menu that contains access to web and mobile formatting. This source code and its supported form are now saved within the Forms page at both the User and Administrator levels.

Once the user has reached the Confirmation page, they are able to copy the single line of code and place it directly into the CSS of the page where they would like for the form to appear. Your signup forms are now powered by Instnt, we'll take care of the rest!

Your Code Is Ready

Copy and paste the following lines of dynamic code into your website where you'd like the generated form to appear.

Web

Div iFrame

Copy code

```
<div id="instnt-form-generator" class="container"></div><script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js">
</script><script>*<![CDATA[*"/var id = 'v374030100000' ; var serviceURL =
'https://service.instnt.org'; $(document).ready(function){$.get(serviceURL
+ "/code/" + id, function(data, status){ $('#instnt-form-
generator').html(data.html)}});/*</script>
```

[Save For Later](#)

[Go To List](#)

Testing Instnt

Getting set up to test Instnt is a three-step process that results in a 60-day production A/B test of a subset of customers signing up for your products or services. The Instnt Customer Success Manager will steward your company through three primary activities: Contracting and Performance, Configuration Validation, and Live Testing and Monitoring.

1. Contracting and Performance

The testing agreement terms, and success metrics will be specified in the Instnt Master Services Agreement (MSA). Instnt requires at least 90 days of production historical data to provide a baseline by which we will be able to compare Instnt's services to the customer onboarding model you currently employ. Instnt is interested in working with your business owners and data scientists to capture statistical metrics and success criteria to determine the false positive rate, fraud actuarial reduction rate, and the abandonment rate. The following table provides examples of the information we will be attempting to capture:

Transactional Metric	Historical 90 Day Data	Instnt's 60 Day Test	Results
Customer Sign up Volume			
True Positive Rate			
False Positive Rate			
Abandonment Rate			
Fraud Labels (Synthetic ID, Third Party, Chargeback)			
Product Annual Lifetime Value			

Maximum Product Loss and Frequency			
Minimum Product Loss Frequency			
Average Product Loss			
Fraud Distribution			
Fraud Rate Seasonality Variable			
Standard Deviation of Product Losses			
Aggregate Annual Loss			
25%, 50%, 75% Quantile of Product Losses			
Annual Revenue			

2. Configuration Validation

Configuration validation will be focused on ensuring integration between Instnt's services and the staged customer website are secure and the information flows between the services are effective. Instnt will provision a dedicated Sandbox for your company with a self-serve dashboard to establish administrators, provision users, and manage your signup forms and workflows.

The Instnt Solution Architecture model below provides a reference to the information flows we support. For illustration purposes Acme.com represents the business site Instnt would be interfacing with, the customer onboarding form is being managed by Instnt at service.instnt.org. For each provisioned onboarding form, Instnt generates a JavaScript snippet configured to make a call to the Instnt form generator REST API function. This involves a cross-site call from within the customer's domain, executed within the customer browser.

Once a customer has been successfully verified, Instnt processes a Decision Callback redirect response routing the customer back into the onboarding workflow. Instnt must supply sufficient information with this redirect for the customer to engage the next step in onboarding the consumer. This reference will take the form of an instntid passed as a base64 encoded query string parameter on the HTTP 302 redirect location. The scheme://host:port/path portion of the redirect location are as supplied by the customer when provisioning the onboarding form.

```
HTTP/1.1 302 Found
Location: https://www.acme.com/onboarding/accept?instntid=MzJGNTYzOTMtQjFCMy00NjAxLTk1REUtQUU0NzkwQjAwMTgyCg==
```

In order to resume their onboarding workflow after the Instnt decision callback, the customer must retrieve the consumer details from the Instnt Get Assertion API using the instntid UUID reference in the Decision Callback payload.

The Get Assertion response will include consumer PII required by the business to onboard the customer, reason codes supporting the decision, and KYC information when applicable. The response will be enclosed in a signed response (in SAML or JWT format) with an encrypted signed Assertion referenced below (SAML example):

```
<?xml version="1.0"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="pfxcab3572-4a31-95cd-8f9b-96c2db72c79c" Version="2.0" IssueInstant="2014-07-17T01:01:48Z"
Destination="http://sp.example.com/demo1/index.php?acs"
InResponseTo="ONELOGIN_4fee3b046395c4e751011e97f8900b5273d56685">
  <saml:Issuer>
    http://idp.example.com/metadata.php
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <ds:Reference URI="#pfxcab3572-4a31-95cd-8f9b-96c2db72c79c">
        <ds:Transforms>
          <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </ds:Transforms>
        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <ds:DigestValue>Z7HTicJySfs//nfe2rPt+3a1CuQ=</ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
    <ds:SignatureValue>...</ds:SignatureValue>
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>...</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </ds:Signature>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
  </samlp:Status>
  <saml:EncryptedAssertion>
    <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmenc#" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
Type="http://www.w3.org/2001/04/xmenc#Element">
      <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#aes128-cbc" />
      <dsig:KeyInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <xenc:EncryptedKey>
          <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmenc#rsa-1_5" />
          <xenc:CipherData>
            <xenc:CipherValue>MjIBuJrQmqgWD5IG0toFuoschHBoGRRHZAht3lAlAA0s4I7L7dhyqSCp8SWPHJZie12d8oTSzh8KfAh0a2ZPkj8PDvIx
QQliRC85zJizM83KmcUc8X6EdapzEP96RR0q6r0A9PkycCEf/E1dz3mO8y7qF4I8eEFGFcLRLGNXdQ=</xenc:CipherValue></xenc:CipherDat
a></xenc:EncryptedKey></dsig:KeyInfo>
        <xenc:CipherData>
          <xenc:CipherValue>...</xenc:CipherValue>
        </xenc:CipherData>
      </xenc:EncryptedData>
    </saml:EncryptedAssertion>
  </samlp:Response>
```

The decoded assertion below is a JSON document containing the above-mentioned fields:

```
{
  "instntid": "32F56393-B1B3-4601-95DE-AE4790B00182",
  "epoch": 1582912190,
  "assertion": "reject",
  "pii": {
    "firstname": "Robert",
    "middlename": "Gabriel",
    "surname": "Mugabe",
    "email": "bobby@spaza.co.zw",
    "mobilenumber": "+2635671234"
  },
  "reason_codes": [ ... ],
  "kyc": {
    "id": "N0HUXBOHUA52RH",
    "name": "Mugabe Robert Gabriel",
    "keywords": [],
    "last_updated_utc": "2020-02-21T10:44:30Z",
```

```

"aka": [{"name": "Robert Mugabe"},
{"name": "Robert Mugabe"},
{"name": "Mugabe Robert Gabriel"},
{"name": "Roberto Mugabe"}],
"assets": [{"public_url": "http://complyadvantage-asset-development.s3.amazonaws.com/13530e09-a2c0-47b9-b72c-5bd75fccb627.pdf",
"source": "complyadvantage",
"type": "pdf"},
{"public_url": "http://complyadvantage-asset-development.s3.amazonaws.com/6c632573-3648-43fd-bc43-35481481cff1.pdf",
"source": "complyadvantage",
"type": "pdf"}],
"associates": [{"association": "Relative", "name": "Bona Mugabe"},
{"association": "Child", "name": "Chatunga Bellarmine Mugabe"},
{"association": "Spouse", "name": "Grace Mugabe"},
{"association": "grandson", "name": "Simbanashe Chikore"}],
"entity_type": "person",
"name": "Political Position", "source": "complyadvantage", "tag": "political_position", "value": "former President of Zimbabwe",
{"name": "Gender", "source": "complyadvantage", "value": "male"},
{"name": "Chamber", "source": "complyadvantage", "value": "African Union"}],
"media": [{"date": "2019-10-01T00:00:00Z",
"snippet": "The Herald No allowances for MDC-A after SONA boycott",
"title": "1kg cocaine lands Peruvian in court | The Herald",
"url": "https://www.herald.co.zw/1kg-cocaine-lands-peruvian-in-court/"}],
"sources": ["tresor-direction-generale",
"dfat-australia-list",
"belgium-consolidated-list-of-the-national-and-european-sanctions",
"swiss-seco-list",
"complyadvantage",
"ofac-sdn-list",
"complyadvantage-adverse-media"],
"types": ["adverse-media",
"adverse-media-financial-crime",
"adverse-media-fraud",
"adverse-media-general",
"adverse-media-narcotics",
"adverse-media-sexual-crime",
"adverse-media-terrorism",
"adverse-media-violent-crime",
"pep",
"pep-class-1",
"pep-class-2",
"pep-class-4",
"sanction"]
}

```




Once we have completed the staging area testing, Instnt will migrate the forms and single line of code to a production facing instance of the customer website that supports the customer onboarding process. Live testing will take 60 days and will take the form of an A/B test. Version B of your website or application will deploy the Instnt code, generating your signup forms for your various onboarding flows. You'll then send 10% or more of your traffic to version B of the site randomly. Fraud and no fraud labels for the population who have signed up through Instnt's variant signup on site B will then be collected over the next 60 days. Instnt will measure the number ratio of good vs risky vs uncategorized, the types of fraud, types of losses and other metrics which enable us to calculate the liability exposure and the baseline for acceptance in your production system. Instnt will then tune the models to indemnify you while increasing the volume of good new customers signed up.