

Confidential

**Business Solution Document**Fidamy\_Compliance Check



# **Change Records**

Date	Author	Version	Note	Reviewer
2025/3/28	Adeline Liu	V0.1	Initial Version	
2025/4/3	Liam, Adeline Liu	V0.2	Update descriptions and pending questions based on comments	
2025/4/8	Adeline Liu	V0.3	Organized whether Graphene blocks/not block the case in the Business Scenarios (2.2.3)	
2025/4/9	Adeline Liu	V0.4	Update Audit related requirement (2.7)     Claim – Registration: Every time when click the "Submit" button in manual flow, we will do the Compliance check. (2.3.4.2)	
2025/4/9	Liam	V1.0	Signoff Version	



# **TABLE OF CONTENTS**

D	ocu	ment H	istory	2		
Ta	able	of Con	itents	3		
1		Introdu	ıction	5		
	1.1					
	1.2	·				
	1.3	1.3 End Users				
	1.4	Gloss	sary·····	5		
2		Busine	ss Solutions	6		
	2.1	Solut	ion Summary·····	6		
	2.2	Overa	all Business Rules·····			
		2.2.1	Tags ·····	6		
		2.2.2	Client ID & Customer ID	7		
		2.2.3	Business Scenarios			
2.3 Fraud C		Frauc	d Check ·····	9		
		2.3.1	Policy Issuance (New Business)	9		
		2.3.2	Policy Issuance + 45 Days ·····	···10		
		2.3.3	POS – Information Change ·····	···11		
		2.3.4	Claim	12		
		2.3.5	Fraud Tag Update (Webhook) ·····	15		
	2.4	Sanc	tion Check	16		
		2.4.1	Policy Issuance (New Business)	16		
		2.4.2	POS – Information Change ····	18		
		2.4.3	POS – Cancellation with Refund ·····	···18		
		2.4.4	Claim	20		
		2.4.5	Sanction Tag Update (Webhook)	···21		
		2.4.6	Sanction Deregistration (Unsubscription)	22		
	2.5	API li	ntegration	23		
	2.6	Turn-	Around-Time (TAT) Notification ·····	23		
	2.7	Audit		24		
		2.7.1	Monthly Reconciliation	24		
		2.7.2	Traceability	24		
3		Appen	dix	24		
4		Refere		24		

### 1 Introduction

### 1.1 OVERVIEW

This document describes the business solution of Compliance Check, including Fraud Check and Sanction Check, for all products.

### 1.2 ASSUMPTIONS

- 1. The compliance checks setup combines Fraud Checks and Sanction Checks. Which, from an operational perspective, are two completely distinct topics.
- 2. Alerts do not trigger immediate rejection in Graphene system. Fidamy operators will manually review and handle any case.
- In Day 1, Policyholder = Insured = Payee = Payer. All compliance checks are conducted on the Policyholder (PH). The "customer" in the following sections refers to Policyholder (PH) in Day 1.
- 4. Fidamy will not allow auto-POS / auto-modification of customer name or customer date-of-birth. Not allowed to change the ownership of the policy.
- 5. The compliance related functions/modules mentioned in this document are based on the latest Graphene system baseline version.

### 1.3 END USERS

Customer.

### 1.4 GLOSSARY

Acronyms	Description

Table 1 Acronyms

### 2 Business Solutions

### 2.1 SOLUTION SUMMARY

Fidamy conducts both fraud and sanction name screenings on the (prospective) customer based on a database of known fraudsters and a number of sanction lists respectively.

The **Fraud Check** is always a one-off, real-time check on the person, while the **Sanction Check** is a one-off, real-time check and enrolment in ongoing monitoring. The Fraud result and Sanction result will be updated in Graphene from the Fidamy Compliance Service, as it gets any updates from the underlying vendor systems.

Fidamy Compliance Service wraps the vendors on Fraud (CIS-FISH) and Sanction (ComplyCube). Graphene integrates with Fidamy Compliance Service for both Fraud and Sanction, including status inquiry and status update.

2.2 OVERALL BUSINESS RULES

### 2.2.1 Tags

1. The status and corresponding outcome of API response:

status	outcome
pending	(will be empty)
failed	not_processed
complete	clear, attention, match_confirmed

#### 2. The Tag values saved in Graphene Customer Center:

Tag Name	Values	
Fraud Tag	pending, failed, clear, attention, match_confirmed	
Sanction Tag	pending, failed, clear, attention, match_confirmed	
Sanction Subscription Tag	subscribed <mark>, unsubscribed</mark>	

**Graphene Customer Center** displays the latest Tag value on frontend, and the Tag change records (history) json is stored in the Graphene backend.

#### 3. Fraud Tag and Sanction Tag handlings:

- a) If Tag = "clear", then **no** need actions.
- b) If Tag does not equal to "clear", i.e., "pending, failed, attention, match\_confirmed", it will require manual input or review by Fidamy staff in the

Commented [LG1]: Adeline, perhaps an idea to refer to the Fidamy system throughout the BSD as "Fidamy Compliance Service" instead of "Fidamy Middleware" to make it more specific?

Commented [沁刘 2R2]: Updated!

Commented [LG3]: Adeline, should we make explicit in the naming that this is sanction subscription tag (i.e., not related to fraud).

Commented [沁刘 4R4]: Can. Have updated it~

Commented [LG5]: Adeline, perhaps these values should be written as completely lowercase (i.e., subscribed, unsubscribed)?

Commented [沁刘 6R6]: Can. Have updated.

Peak3 Limited

6



underlying vendor systems (i.e., CIS-FISH and ComplyCube). Once these alerts are handled, the status will be updated in the Fidamy Compliance Service. Which will subsequently inform Graphene through webhook. During this process, Alert Notifications to instruct the handling will be sent by the Fidamy system or vendor systems (CIS-FISH or ComplyCube).

c) If the updated Tag = match\_confirmed, Fidamy will escalate the case to NN, based on the input from NN, Fidamy may manually cancel the policy in the Graphene system without a refund or take other steps.

#### 4. Sanction Subscription Tag:

- "subscribed" means ongoing monitoring on Sanction result. Fidamy Compliance Service will keep monitoring on the client and send the updated Sanction result via a Webhook. See 2.4.5 Sanction Tag Update.
- "unsubscribed" means no ongoing monitoring.
- 5. When generating the Proposal (Application), Graphene will also create the customer in Graphene Customer Center if there are no existing customer in the system with the identical Customer Uniqueness values (See Customer Uniqueness documentation for exact values). Fraud Tag, Sanction Tag and Sanction Subscription Tag will be empty. Will not trigger any Compliance Check at this point, nor notifications.

### 2.2.2 Client ID & Customer ID

### 1. Definition:

- a) <u>Client ID</u>: the internal client id from ComplyCube for sanction name screening. This value is unique for each customer in the ComplyCube system. There is no Client ID for fraud name screening in the CIS-FISH system.
- b) <u>Customer ID</u>: The Graphene Customer ID reference towards both the sanction name screening in ComplyCube and the fraud name screening in CIS-FISH.
- 2. When changing personal information, keep the **same** Customer ID in Graphene and the **same** Client ID in ComplyCube.
- 3. If the original client is "unsubscribed", i.e., ongoing monitoring = False. Later, this same person purchases a new policy again. Then, we will use the same customer ID in Graphene and keep the same Client ID in ComplyCube. Graphene calls Sanction Check Create API and updates the corresponding Tags.

Commented [沁刘 7]: Question for later reply:

If Fraud / Sanction validation fails, i.e., it is indeed a
terrorist, from Business perspective, how will Fidamy
handle this policy in Graphene system? For example,
manually cancel the policy in Graphene with full refund,
with a specific Cancellation Reason? Or partial refund?

Understand that this scenario will never occur, or rarely occur. However, just want to know whether the "Cancellation" function can satisfy the handlings.

Commented [LG8R8]: Please see answer in track changes. If someone is sanctioned, Fidamy cannot have any financial relation with the person/entity. So, we are never allowed to do any sort of refund or payout to them. We will freeze their policy, go to NN, and the Dutch government regulator to get instructions on how to proceed.

### 2.2.3 Business Scenarios

The following Business Scenarios will conduct Fraud and Sanction Checks:

Scenarios	Sub Scenarios	Fraud Check	Sanction Check
New Business	"unsubscribed" or empty	Fraud Check API	Sanction Check – Create API (Not block)
Policy Issuance	"subscribed"	(Not block)	N/A
Policy Issuance + 45 Days		Fraud Check API	N/A
DOS	Policyholder Basic Information Change	Fraud Check API (Not block)	Sanction Check – Update API (Not block)
POS	Cancellation	N/A	Internal Sanction Check (block)
	Registration if "unsubscribed"	Fraud Check API	Sanction Check – Create API (block)
Claim	Registration if "subscribed"	(block)	Internal Sanction Check (block)
	Approval	Internal Fraud Check (block)	Internal Sanction Check (block)
Tag Update		Fraud Result Update API	Sanction Result Update API
Unsubscribe		N/A	Sanction Check – Monitoring API

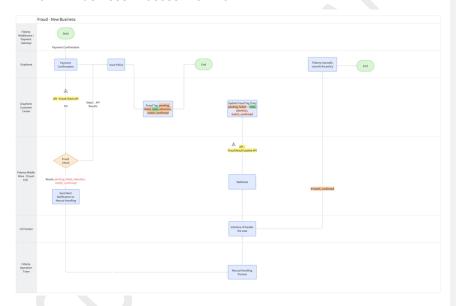
<u>Note:</u> "block" means Graphene turns to manual flow or pops up soft reminder.

#### 2.3 FRAUD CHECK

Fidamy performs the Fraud Name Screening on the customer at four critical processes: Policy Issuance, Policy Issuance + 45 Days, Policy Modifications (Policyholder Basic Information Change in Day 1), and Claim. The processes use the **Fraud Check API** to enquiry the Fraud result from Fidamy Compliance Service and the **Fraud Result Update API** (Webhook) to update results in **Graphene Customer Center**.

### 2.3.1 Policy Issuance (New Business)

### 2.3.1.1 Business Process Workflow



### 2.3.1.2 Step Descriptions

- After payment confirmation, Graphene triggers Fidamy Compliance Service Fraud Check API to validate the policyholder (PH). Graphene uses <u>Graphene Customer</u> <u>ID</u> as <u>customerId</u> in API request.
- Graphene updates the Fraud Tag in Customer Center with the API response.
   See Overall Business Rules 2.2.1 Tags.
- 3. Compliance checks will **not** block Policy Issuance. Graphene will issue the policy after Fraud Check.

Commented [LG9]: Not entirely sure what is meant with "in Day 1" here

Commented [沁刘 10R10]: Day 1 means when first launch this requirement.

For some complex requirements, we may split the release into Day 1, Day 2, .... in order to catch up with the go-live of the base requirements, or maybe some requirement are not needed at first.

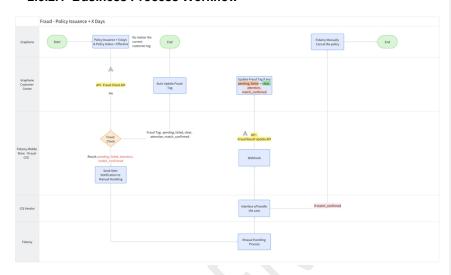
So in Day 1, when we first launch, maybe we will launch some parts of the requirement. Then in Day 2, with a later release date, we may have more scopes. (The Day 2 release will not have any impacts on normal operation of the production environment.)

Commented [LG11]: Adeline, we have renamed this field to 'externalld' to align it with sanction name screening naming conventions. @Bala Narayanan will update this in the Fidamy Compliance Service APIs shortly

Commented [沁刘 12R12]: Sure. Updated!

### 2.3.2 Policy Issuance + 45 Days

### 2.3.2.1 Business Process Workflow



### 2.3.2.2 Step Descriptions

- After 45 Days from Policy Issuance, Graphene triggers Fidamy Compliance Service Fraud Check API to validate the policyholder (PH).
- 2. Batch Job:
  - a) Batch Job Time: 04:00 AM UTC
  - b) Object Policy Status: Effective
  - c) Scope: Policy Issuance Day + 45 Days within intraday 00:00:00~23:59:59
  - d) Subject: Policyholder (PH)
- Graphene updates the Fraud Tag in Customer Center with the API response.
   See Overall Business Rules 2.2.1 Tags.

'Policy Issuance Day + n' (n= 45 for Day 1) and batch job time are configurable backend in nacos configuration center. Future requirements may change the 'Policy Issuance Day + n' and batch job time.

<u>Note:</u> This check is conducted <u>by policy</u>. No matter how many policies the same client has, we will process this check for each policy.

<u>For example</u>, one customer has policy A with Policy Issuance Date = 2025/2/1, policy B with Policy Issuance Date = 2025/3/5.

Commented [沁刘 14R14]: Suggest to be around 3-4AM

Commented [LG15R14]: Let's go with 04:00 UTC

Commented [沁刘 13]: Pending

Commented [LG16]: Adeline, what does 'NACOS' mean?

Commented [沧刘 17R17]: "nacos" is like the "configuration center" for codes. Normally used for some data configurations such as database information, batch job information, api information, etc In order to avoid frequent changes to the project codes, such configurations are unified into "nacos" management.

Commented [LG18]: @Matthijs Kierkels, please

Commented [LG19R19]: Need to double check that we do fraud name screening for existing active policyholders and also the +45 day check for these policyholders

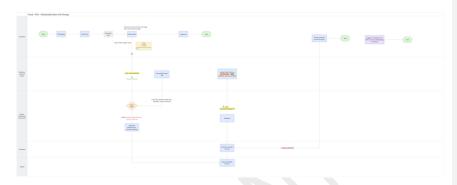
Commented [MK20R19]: Correct!



System will perform the check for the customer on 2025/2/1 + X Days (policy A), also perform check on 2025/3/5 + X Days (policy B).

### 2.3.3 POS - Information Change

#### 2.3.3.1 Business Process Workflow



### 2.3.3.2 Step Descriptions

 Fidamy Operators / Customers change personal information via Policyholder Basic Information Change POS Item.

#### 2. Stages and Validations:

- Automatic Flow: When POS case automatically enters the <u>Confirmation</u> Stage
- Manual Flow: When click the "Submit" button on Confirmation Stage,

if any of

- a) First Name
- b) Last Name
- c) Residence Country
- d) Date of Birth

is changed, Graphene triggers Fidamy Compliance Service **Fraud Check API** to validate the policyholder (PH). Other field changes will **not** trigger Compliance checks.

<u>Note:</u> Compliance checks are the last check that is done. Only after other business rules are passed, will conduct Compliance checks.

Commented [LG21]: Important that this check is the last check that is done. If the POS request is already blocked by a business rule earlier, it should never call fraud nor sanction. Otherwise the data may become inconsistent.

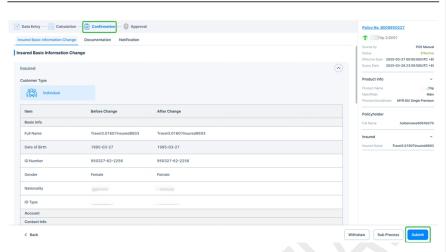
Commented [沧刘 22R22]: Yes. We will configure other rules in the earlier stages: Registration, Data Entry, Calculation. Then, only after all other rules are passed, will conduct the Compliance check at Confirmation Stage.

Also included the statements in content. See the copywritings in red.

Peak3 Limited

11





- 3. Graphene updates the **Fraud Tag** in **Customer Center** with the API response. See **Overall Business Rules 2.2.1 Tags**.
- 4. After retrieving the API response, no matter what the result is, Graphene continues the POS process, will **not** have any blocks.

<u>Note:</u> Only after POS case is completed (which is not blocked by the Fidamy Compliance Service API), will Graphene update the changed personal information for this policy as well as for this customer in **Customer Center**.

### 2.3.4 Claim

### 2.3.4.1 Business Process Workflow



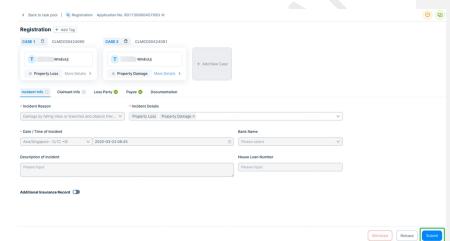
#### 2.3.4.2 Step Descriptions

During the claim process, Graphene conducts Compliance Check during two stages:

- Immediately when claim case is made: Registration Stage
- Before claim completion and claim payout: Approval Stage

#### A. Registration Stage:

- 1. Check starts:
  - Automatic Flow: When claim case automatically enters the Registration Stage,
  - Manual Flow: When click the "Submit" button on <u>Registration Stage</u> (and moves to next stage),

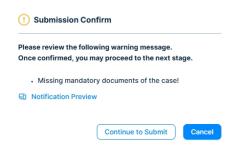


Graphene triggers Fidamy Compliance Service **Fraud Check API** to validate the policyholder (PH).

<u>Note:</u> Every time <u>when click the "Submit" button in manual flow,</u> we will do the Compliance check.

- 2. After retrieving the API response,
  - a) If Tag = "clear", then no need actions. Graphene will continue the claim flow.
  - b) If Tag does not equal to "clear", i.e., "pending, failed, attention, match\_confirmed", then Graphene will
  - Automatic Flow: turn it into a manual flow. The Claim case status will be
     "Waiting for Registration" in the claim public task pool. Fidamy Claim operator
     needs to manually pick up the case from Application Pool and "Submit" for the
     Registration Stage.
  - Manual Flow: pop up the soft reminder:





Error message: WARNING: There was a fraud alert related to this claim. Please handle this case before proceeding.

Claim operator can click "Continue to Submit" to continue to next stage,

Or click "Cancel" to stay in Registration stage and waiting for further actions. Claim case status = "Registration in Progress". After further checks, Fidamy Claim operator manually continues the claim case for Registration stage.

 Graphene updates the Fraud Tag in Customer Center (record tracking) with the API response. See Overall Business Rules – 2.2.1 Tags.

#### B. Approval Stage:

- 1. Check starts:
  - Automatic Flow: When claim case automatically enters the Approval Stage,
  - Manual Flow: When click the "Submit" button on Approval Stage,

Graphene triggers **Internal Fraud Check** to get the latest Fraud Tag of Policyholder (PH) from **Customer Center**.

- 2. After retrieving the response,
  - a) If Tag = "clear", then no need actions. Graphene will continue the claim flow, complete the claim process and process claim payout.
  - a) If Tag does not equal to "clear", i.e., "pending, failed, attention, match\_confirmed", then Graphene will
  - Automatic Flow: turn it into a manual flow. The Claim case status will be "Waiting for Approval" in the claim public task pool. Fidamy Claim operator needs to manually pick up the case from Claim Case Pool and "Submit" the Approval Stage.
  - Manual Flow: pop up the soft reminder:

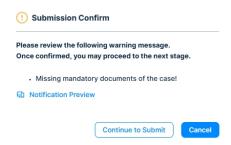
Commented [沁刘 23]: Please help provide the reminder message.

Commented [LG24R24]: @Matthijs Kierkels any thoughts here? Perhaps: "WARNING: There was a fraud alert related to this claim. Please handle this case before proceeding".

Commented [MK25R24]: It helps if you can see what it concerns, fraud or sanctions. See happy to do it as you suggest.

Commented [沁刘 26R24]: Please see the updated error message.





Error message: WARNING: There was a fraud alert related to this claim. Please handle this case before proceeding.

Claim operator can click "Continue to Submit" to continue the next step,

Or click "Cancel" to stay in Approval stage and waiting for further actions. Claim case status = "Approval in Progress". After further checks, Fidamy Claim operator manually continues the claim case for Approval stage.

<u>Note:</u> Every time when click the "Submit" button at Approval Stage, will call the internal check and check the **latest** Tag in Graphene **Customer Center**.

### 2.3.5 Fraud Tag Update (Webhook)

After careful investigation of "pending, failed", Fidamy Compliance Service will trigger Graphene Fraud Result Update API. Graphene automatically updates the Tags in Graphene Customer Center (record tracking). Will not trigger notification to customer.

Commented [沁刘 27]: Please help provide the reminder message.

Commented [LG28R28]: @Matthijs Kierkels any thoughts here? Perhaps: "WARNING: There was a fraud alert related to this claim. Please handle this case before proceeding".

Commented [MK29R28]: It helps if you can see what it concerns, fraud or sanctions. See happy to do it as you suggest.

Commented [沁刘 30R28]: Please see the updated error message.

Commented [LG32R32]: 
Matthijs Kierkels any thoughts here? Perhaps: "WARNING: There was a fraud alert related to this claim. Please handle this case

Commented [MK33R32]: Same answer as above.

before providing claim case approval".

Commented [沧刘 34R32]: We will suggest that we use some more "general" wording, which will help increase the resue rate and save efforts.

We will suggest that we use the same message as Registration Stage:

WARNING: There was a fraud alert related to this claim. Please handle this case before proceeding.

Commented [沧刘 31]: Please help provide the reminder message.

#### 2.4 SANCTION CHECK

Sanction Check is another core component of Fidamy's compliance process, designed to ensure individuals and entities are screened against relevant sanction lists. Sanction Check includes both a one-off inquiry and continuous daily monitoring. Termination of monitoring occurs when a customers' policies as "PH" have been terminated > 6 months. Graphene integrates with Fidamy Compliance Service to receive Sanction results and to update the Sanction Tag in Graphene.

### 2.4.1 Policy Issuance (New Business)

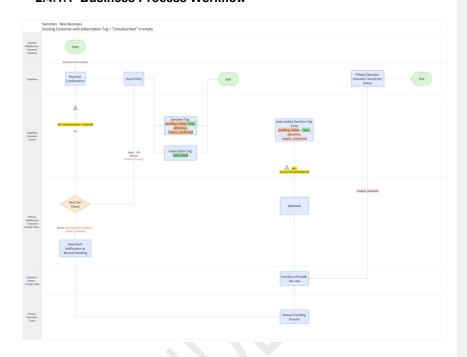
Since Sanction Check includes both a one-off inquiry and continuous daily monitoring, when first issue the policy for New Business, only needs to conduct Sanction Check for the "**New**" customers, i.e., customers without active sanction monitoring.

#### "New" customers:

- Customer with Sanction Subscription Tag is empty: When generate the Proposal, if the customer is a new customer, Graphene will create the customer in Graphene Customer Center with empty Sanction Subscription Tag. For these customers, no ongoing monitoring, needs to conduct Sanction Check.
- 2) <u>Customer with Sanction Subscription Tag = "unsubscribed</u>": The existing customers' all policies has been terminated > 6 months, and the customer Sanction Subscription Tag is now "unsubscribed". At this time, the customer purchases a new policy. Then, needs to restart the Sanction check.

For the existing customer in **Graphene Customer Center** with **Sanction Subscription Tag** = "subscribed" (Fidamy ongoing monitoring = True), which means there is already ongoing Sanction monitoring via Webhook, **no need** to conduct Sanction Check.

## 2.4.1.1 Business Process Workflow



### 2.4.1.2 Step Descriptions

- After payment confirmation, if customer Sanction Subscription Tag =
   "unsubscribed" or is empty, Graphene triggers Fidamy Compliance Service
   Sanction Check Create API to validate the policyholder (PH). Graphene uses
   Graphene Customer ID as customerId in API request.
- Graphene updates the Sanction Tag in Customer Center with the API response.
   See Overall Business Rules 2.2.1 Tags.
- Graphene updates the Sanction Subscription Tag in Customer Center as "subscribed"
- Compliance checks will not block Policy Issuance. Graphene will issue the policy after Sanction Check.

<u>Note:</u> For the existing customer but **Sanction Subscription Tag = "unsubscribed"**,

- 1) Use the existing Graphene Customer ID as customerId.
- 2) Graphene updates the status to "subscribed" (record tracking).

ComplyCube will not create a new Client in ComplyCube, but will create a new check under that existing ComplyCube Client.

### 2.4.2 POS - Information Change

#### 2.4.2.1 Business Process Workflow



### 2.4.2.2 Step Descriptions

All steps are the same as Fraud – POS – Information Change. Please refer to **Section 2.3.3.2**.

Difference: API is Sanction Check - Update API.

Once the information is updated, a new check will be created in Fidamy Compliance Service and the check status will be received via a Webhook, see **Section 2.4.5 Sanction Tag Update**.

### 2.4.3 POS – Cancellation with Refund

### 2.4.3.1 Business Process Workflow



Commented [沁刘 35]: If cancellation with no refund, still need internal Sanction check?

Commented [LG36R36]: In the case where a policy gets cancelled with no refund (e.g, the customer turns off auto-renewal prior to renewal date). There is no need for an additional sanction check.

The sanction check at cancellation is intended to safeguard against sending money to sanctioned individuals. If there is no cash transaction, we do not need to do sanction check.

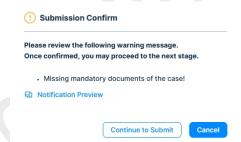
@Matthijs Kierkels can you please confirm?

### 2.4.3.2 Step Descriptions

- 1. Sanction Check conducts on the Confirmation Stage.
- 2. Check starts:
  - Automatic Flow: When POS case automatically enters the <u>Confirmation</u> <u>Stage</u>,
  - Manual Flow: When click the "Submit" button on <u>Confirmation Stage</u> (and moves to next stage),

Graphene triggers Internal Sanction Check to get the latest Sanction Tag of Policyholder (PH) from Customer Center.

- 3. After retrieving results:
  - a) If Tag = "clear", then no need actions. Graphene will continue the POS flow, complete the POS process and process the refund.
  - b) If Tag does not equal to "clear", i.e., "pending, failed, attention, match confirmed", then Graphene will
  - Automatic Flow: turn it to a manual flow. The POS case status will be
     "Waiting for Data Entry" in the POS Task Pool. Fidamy POS operator needs
     to manually pick up the case and "Submit" the Data Entry, Confirmation
     stages.
  - Manual Flow: pop up the soft reminder:



Error message: WARNING: There was a sanction alert related to this POS. Please handle this case before proceeding.

POS operator can click "Continue to Submit" to continue the submit,

Or click "Cancel" to stay in Confirmation stage and wait for further actions. POS case status = "Data Entry in Progress". After further checks, Fidamy POS operator manually continues the manual POS for Confirmation stage.

<u>Note:</u> Every time when click the "Submit" button at <u>Confirmation Stage</u>, will check the latest Tag from Graphene **Customer Center**.

Commented [沁刘 37]: Pending

Commented [LG38R38]: Please align with fraud error message, replacing fraud mention with sanction

Commented [沁刘 39R38]: Please see the updated error message.

### 2.4.4 Claim

#### 2.4.4.1 Business Process Workflow



### 2.4.4.2 Step Descriptions

During the claim process, Graphene conducts Compliance Check during two stages:

- Immediately when claim case is made: Registration Stage
- Before claim completion and claim payout: Approval Stage

### A. Registration Stage:

The process are similar to Fraud - Claim, refer to Section 2.3.4.

### Differences:

- 1. Subject and APIs:
  - a) If Sanction Subscription Tag = "subscribed", Graphene triggers internal Sanction Check to validate PH from Graphene Customer Center.
  - b) If Sanction Subscription Tag = "unsubscribed", Graphene triggers a Onetime Sanction Check - Create API to validate PH. Graphene updates the Sanction Tag in Customer Center (record tracking) with the API response. Graphene will not update the Sanction Subscription Tag.
- 2. Pop up Error message: WARNING: There was a sanction alert related to this claim. Please handle this case before proceeding.

#### B. Approval Stage:

Same as Fraud - Claim, refer to Section 2.3.4.

Differences:

Commented [沁刘 40]: Pending

Commented [LG41R41]: Please align with fraud error message, replacing fraud mention with sanction mention

Commented [沁刘 42R41]: Please see the updated error message.



- 1. Checks: Internal Sanction Check
- 2. Pop up Error message: WARNING: There was a sanction alert related to this claim. Please handle this case before proceeding.

<u>Note:</u> Here no need to differentiate the "subscribed" and "unsubscribed" customers since for the "unsubscribed" customers, the Tag in Customer Center will also be updated after Registration Stage check and Webhook update.

### 2.4.5 Sanction Tag Update (Webhook)

#### 2.4.5.1 Business Process Workflow



Sanction keeps monitored and updated via a Webhook.

- 1) After careful investigation of "pending, failed",
- 2) During regular Sanction Webhook monitoring,

Fidamy Compliance Service will trigger Graphene **Sanction Result Update API** to return a Webhook. Graphene automatically updates the **Tags** in Graphene **Customer Center** (record tracking). Will **not** trigger notification to customer.

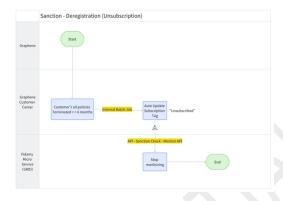
Commented [沁刘 43]: Pending

Commented [LG44R44]: Please align with fraud error message, replacing fraud mention with sanction

Commented [沁刘 45R44]: Please see the updated error message.

### 2.4.6 Sanction Deregistration (Unsubscribe)

#### 2.4.6.1 Business Process Workflow



#### 2.4.6.2 Step Descriptions

Fidamy requires that customers remain in ongoing sanction monitoring for 6 months after their last policy is terminated.

- If all the policies under the customer as "PH" have been terminated > 6 months, then Graphene runs internal batch job to update Sanction Subscription Tag to "unsubscribed" (record tracking).
- 2. Batch Job:

Suppose Batch job conducts on Day N.

- a) Batch Job Time: 04:00 AM UTC
- b) <u>Subject:</u> Customer under whom all the policies as "PH" have been terminated > 6 months
- c) <u>Scope:</u> Last Policy Termination Date + 6 months within N-1 Day 00:00:00~23:59:59
- d) Action: Update Sanction Subscription Tag to "unsubscribed" in Graphene Customer Center.

"6 months" are configurable backend in nacos configuration center. Future requirements may change the "6 months".

After updating Sanction Subscription Tag to "unsubscribed" in Graphene Customer Center, Graphene triggers Fidamy Compliance Service Sanction Check - Monitoring API immediately to inform Fidamy Compliance Service to stop monitoring. Fidamy Compliance Service will update the "Ongoing Monitoring" to False and stop monitoring.

Commented [沦刘 47R47]: Suggest to be around 3-4AM

Commented [LG48R47]: 04:00 AM UTC is good Commented [沙刘 46]: Pending

Commented [LG49]: Adeline, what is meaning of Nacos?

Commented [沁刘 50R50]: See above explanations.

### 2.5 API INTEGRATION

#### **API List**

No.	Fraud / Sanction	Internal / External	API	Provider
1	- Fraud	External	Fraud Check API	Fidamy Compliance Service
2		Internal	Internal Fraud Check	Graphene
3		External	Fraud Result Update API	Graphene
4	- Sanction	External	Sanction Check – Create API	Fidamy Compliance Service
5		External	Sanction Check – Update API	Fidamy Compliance Service
6		Internal	Internal Sanction Check	Graphene
7		External	Sanction Result Update API	Graphene
8		External	Sanction Check – Monitoring API	Fidamy Compliance Service

#### **API Document**

Please refer to the postman and API spec.

#### Internal Fraud Check & Internal Sanction Check:

Fulfilled by Graphene Decision Engine rules.

# 2.6 TURN-AROUND-TIME (TAT) NOTIFICATION

Each POS / Claim case has a target Turn-Around Time (TAT). When a POS / Claim case has been ongoing for several days, and nearing the target TAT or the target TAT has breached, Graphene will automatically send an email notification to the current operator(s) or supervisor. This email notification is used to remind the POS / Claim user for further actions. Target TAT is different by Goods. Notification templates can be configured by goods level, with / without current POS / Claim operator, nearing / breached target TAT.

Detailed TAT Notification rules will be explained in the TAT Notification BSD.

Commented [沧刘 51]: If Fraud & Sanction check will not block POS process, do we still need the notification when POS case has been pending for more than X days.

Commented [沧刘 52R52]: This is designed as the "POS Turn-and-Time (TAT)". Once POS whole case status is pending for more than X days, will trigger reminder notification to POS user.

Commented [沁刘 53R52]: The other feasible business scenarios for POS TAT notification are: The POS operator hasn't finished the POS case; POS Approval stage needs another operator; etc.

Commented [沧刘 54R52]: If need to have POS TAT Notification, after? days should we trigger the notification? – This can be provided later.

Commented [沧刘 55R52]: Similarly, we have the Claim TAT Notification, after ? days should we trigger the notification? - This can be provided later.

Commented [LG56R52]: Adeline, I think it would be good to have the notifications from Graphene. That way we ensure nothing 'slips through the cracks' and everything is handled promptly.

Commented [LG57R52]: @Matthijs Kierkels, can you make a suggestion after how many days there should be a handling reminder notification for:
- claim cases

- POS / modification cases

Commented [LG58R52]: Perhaps each 3 days?

Commented [沧刘 59R52]: Great. Later when we launch a product, we will include TAT Notification into Function List scope. We can discuss further details based on the specific product, product type and so on.

Commented [沁刘 60]: Details TBD.

Commented [LG61R61]: Adeline, that sounds good!



### **2.7 AUDIT**

Future audit data requirement is still to be finalized. But in general, it comes down to Fidamy being able to carries out a periodic export of the related data to carry out monthly reconciliation with the Fidamy Compliance Service data and the data from the underlying vendor systems (i.e., CIS-FISH and ComplyCube) and Graphene.

### 2.7.1 Monthly Reconciliation

Graphene updates monthly Reconciliation data for **all existing customers** to Fidamy S3 bucket:

s3://fidamy-data-platform-landing-zone/

incoming/

<YYYYMMDD>-reconciliation/
CUSTOMER-SCREENING.PARQUET

Reconciliation data will include customer ID, client ID, policy No., latest Fraud Tag, latest Sanction Tag, latest Sanction Subscription Tag. See Compliance Monthly Reconciliation Data file.

### 2.7.2 Traceability

Graphene saves the change logs of Fraud Tag and Sanction Tag, which will be used for problem troubleshooting when mismatch in Reconciliation or other technical issues.

### 3 APPENDIX

### 4 REFERENCES

/

Commented [沧刘 62]: Future audit data requirement is TBD.

Commented [沧刘 63R63]: Peak3 will provide some samples.

Commented [LG64R63]: See provisional answer in track changes