trunarrative

Exactly who, what and when

TruBank: External Fraud Risk Appetite Statement

This template is provided by TruNarrative to assist financial crime professionals in formulating an 'External Fraud Risk Appetite Statement'. The contents are based on the author's experience in defining fraud practices in banking and financial services. Elements of this template have also received best practice recognition from a leading international auditing firm.

For further assistance or to discuss formulating your firm's risk appetite statement please contact evaughan@trunarrative.com

TABLE OF CONTENTS

Introduction

This template document has been produced with the intention of assisting financial crime risk professionals with defining and documenting their organisations risk appetite for external fraud.

Whilst primarily this template is most suited to those regulated firms involved in core financial activities, such as lending, the sentiment and underlying structure has applications across all aspects of financial crime management and wider requirements of governance documentation.

The author of this document has previously held positions as a Future Fraud Strategy Risk Manager at a major UK bank, as well as the UK Financial Crime Manager at a leading retail partner finance and direct to consumer lending bank.

Document purpose

This section should describe the purpose of the document.

The below statement could be used as a guide...

The purpose of this document is to provide a detailed description of TruBank's 'External Fraud Risk Appetite Statement'. This document should be read in conjunction with TruBank's 'Fraud Policy Document' which contains further detailed information on the internal processes, responsibilities and operational procedures for fraud management.

Note that TruNarrative will separately be publishing a 'best practice guide' for writing a Fraud Policy Document.

What is external fraud risk appetite?

This section should contain a documented statement about what your organisation considers to be 'fraud risk appetite' and who owns the process. A well positioned and defined statement should set the scene for the reader and demonstrate that you have a holistic understanding of what risk appetite is.

The below statement could be used as a guide...

It is often said that no company can make a profit without taking a risk. The same is true for all organisations: no organisation, whether in the private, public or third sector can achieve its objectives without taking risk. The only question is how much risk do they need to take?

External fraud risk appetite is not just about making a statement of how much money TruBank is prepared to lose resulting from fraud on the products and services that we offer to consumers. Whilst such quantitative expressions are a key element, external fraud risk appetite additionally needs to contain qualitative expressions, which reflect TruBank's internal stance and culture in preventing, detecting and responding to external fraud incidents.

There continues to be a rise in external fraud related incidents within banking and financial services as a whole. Data breaches, which result in identity theft often lead to a wide range of fraud risks, but primarily the continued rise of impersonation fraud poses challenges for all regulated firms, including TruBank. Other fraud related risks, such as those who have no intention repay and or honour financial agreements continue to be prevalent in the risk landscape.

In light of the increasing frequency and complexity of external fraud related incidents, there is a need to have a comprehensive risk appetite framework in place at TruBank that helps to understand and manage risk. Risk appetite is more than a sophisticated key performance indicator (KPI) for risk management. It's the core instrument for better aligning TruBank's resource allocation, reporting and investment within the fraud and financial crime domain.

Ownership and management of external fraud risk appetite

This section should describe who owns and administers external fraud risk appetite. The ownership of risk appetite should be at an appropriate senior level. Dependent on the size of the firm the management of the appetite may be separate from the overall owner. Regardless, relevant stakeholders in the decision making process should be documented.

The expressions of risk appetite (see below) should not be made in isolation, but rather with key internal stakeholders, which may include Product Owners, Risk, the Financial Crime Manager and Finance. This holistic view of external fraud risk appetite ensures a collective expression from both a qualitative and quantitative perspective. More importantly, it aligns and manages the impact of fraud losses with P&L, compliance requirements as well as customer experience.

The statement should be approved by the firms board.

The below statement could be used as a guide...

External fraud risk appetite is owned by TruBank's Financial Crime Director who reports directly to the Board who have ratified the statement. Further, fraud risk appetite is managed on a daily basis by TruBank's Head of Fraud Strategy who oversees the resource, systems and controls in place to prevent, detect and respond to fraud.

The expressions of risk appetite are defined as:

1. The amount of material losses that TruBank is willing to accept in pursuit of our commercial objectives. and;
2. The tolerance (the maximum material loss that TruBank is willing to accept before we either (a) revisit the appetite or (b) instigate further preventative measures.

External Fraud Risk Appetite Statement

This section should contain the full description of the firms External Fraud Risk Appetite Statement and how it relates to the products and services that it offers to consumers. The way in which it is defined in the context of triggers and tolerance will vary and will be dependent on how the firm operates.

Appetite, tolerance and triggers

Consideration now needs to be given as to how the firm will define its 'appetite' - what is the appetite for fraud losses and how should this be defined?

For example, should the firm set the overall fraud loss appetite as:

(a) an overall monetary figure of loss across every product line that impacts the firm's P&L?
(b) a monetary figure of loss that relates to an individual product line?
(c) a monetary figure of loss by various channels?
(d) a fixed number of external fraud incidents that a firm identifies across all product lines?
(c) a fixed number of external fraud incidents that a firm identifies in one specific product line?

The truth is there is no right or wrong way to define this. However, the critical measure of this is the ability to be able to set a value that enables the firm to identify a trigger point as to when it needs to take action.

A risk appetite statement should be clear in communicating what is acceptable and what is not. By providing a clear threshold and measure enables incidents to be managed proportionately. More importantly it provides a framework for fraud professionals to work within.

In the below example we will use TruBank, which only has only one product (an interest bearing personal loan). Should a firm have a number of products this methodology could be expanded or the best suited appetite measure from points a-c adopted based upon the commercial model.

TruBank's 2019 External Fraud Risk Appetite Statement has been approved by the Board. TruBank has a low external fraud risk appetite and fully commits to maintaining an appropriately skilled and dedicated business function to detect and respond to external fraud incidents.

TruBank defines it's risk appetite for fraud losses as:

Confirmed fraud losses not exceeding the specified percentage (see table) of credit exposure, derived from the personal loan portfolio, within a two month rolling cycle. Additionally, TruBank has a tolerance level to external fraud which shall not exceed the specified percentage (see table) of credit exposure within the same defined criteria as risk appetite.

Product	Fraud Risk Appetite	Within Tolerance	Over Tolerance
TruPersonal Instant Loan	0.00% to <=0.25%	>0.25% to <=0.30%	>0.30%
This the only product that TruBank has	*Fraud losses against this percentage is tracked daily and reported on regularly. The impact can be seen within the P&L in real-time*	*This figure acts as the trigger point for review of fraud losses*	*Remediation action and escalation must have occurred if fraud losses get to this point*

Should on-going monitoring identify that the tolerance has been surpassed (see table), then the relevant product owner shall be informed and the matter escalated to the Fraud Risk Committee who shall make a decision as to whether risk appetite and tolerance is increased, or remedial measures are implemented to mitigate the increasing risk to the profitability of the product portfolio

Compliance and risk management

As discussed a comprehensive External Fraud Risk Appetite Statement is just not making a statement of how much money a firm is prepared to lose resulting from fraud. The statement also needs to reflect a firms internal stance and culture in preventing, detecting and responding to external fraud incidents.

The below statement could be used as a guide…

TruBank places great emphasis on protecting its income streams as well preventing further harm to the victims of crime arising from external fraud incidents. To maintain performance in-line with the accepted external fraud risk appetite, and with a focus on protecting victims of crime, TruBank commits to maintaining a dedicated and appropriately skilled team to manage financial crime risk. This team, which overseen by the Head of Fraud Strategy shall be responsible for reporting performance against risk appetite on a monthly basis to key stakeholders and quarterly to the Fraud Risk Committee.

TruBank shall comply with all relevant regulations and syndicated membership rules, and has no appetite for regulatory or membership breaches. TruBank has policies, procedures and risk assessments in place to ensure compliance with regulatory and other obligations, and robust oversight and monitoring to evidence compliance through the governance structures identified in the Fraud Policy Document.

TruBank's culture in regards to fraud prevention is one of engagement and information sharing and we achieve this through external industry forums to proactively identify and manage associated risks. In addition, TruBank fully complies with all regulatory and law enforcement requirements for disclosure of external fraud related information.

Management of External Fraud Risk Appetite

Reporting

External fraud risk management is underpinned by effective management information. TruBank has a unified financial crime platform that is provided by TruNarrative. This platform provides the single point of fraud decisions and investigation for all incidents relating to external fraud. The platform solution brings fraud

detection, identity verification, eKYC and AML compliance into a single easy-to-configure environment accessed via a single API.

Performance against risk appetite is monitored in real-time in TruNarrative's platform and is displayed in the MI dashboard functionality of the platform. Further data from the platform is ingested back into TruBank's 'big data environment' via the real-time API and also web-hooks. This enables TruBank to have a real-time holistic view of all financial crime risk.

About TruNarrative

We founded TruNarrative with a clear goal: **to make safe commerce simpler**. Safe commerce is simpler when IDV, AML and fraud checks run in a single financial crime platform. Simpler for consumers, simpler for you.

With a successful track record in the ID and fraud market, the TruNarrative leadership team brings over 100 years combined experience in the data and technology space. Through corporate partnership with a USA-based holdings group, we have the financial and technology resources for long term success.

With offices in Leeds, London, New York, Singapore and Hong Kong we are a truly International business, solving Global challenges. We serve market stalwarts and new entrants and we add value wherever fraud risk and compliance risk arise from online and in-store interactions. Companies in a range of sectors adopt TruNarrative.

The spread of eCommerce and the rise of fintech require a fresh approach to fraud and money laundering detection and prevention. The new approach harnesses artificial intelligence, in data-rich systems capable of learning. Legacy systems cannot evolve quickly enough to deliver. That's why we used our decades of direct experience to create a new platform. The TruNarrative platform contains a proven decision engine built by an established technology team.

Legacy technology constrains current IDV, KYC, Fraud and Money Laundering detection systems. Without an integrating platform, each data set and subsequent decisions exist in a silo. Silos create inefficiencies and add to manual work. This adds delays that impinge on customer experience and creates unnecessary management costs right across an organisation.

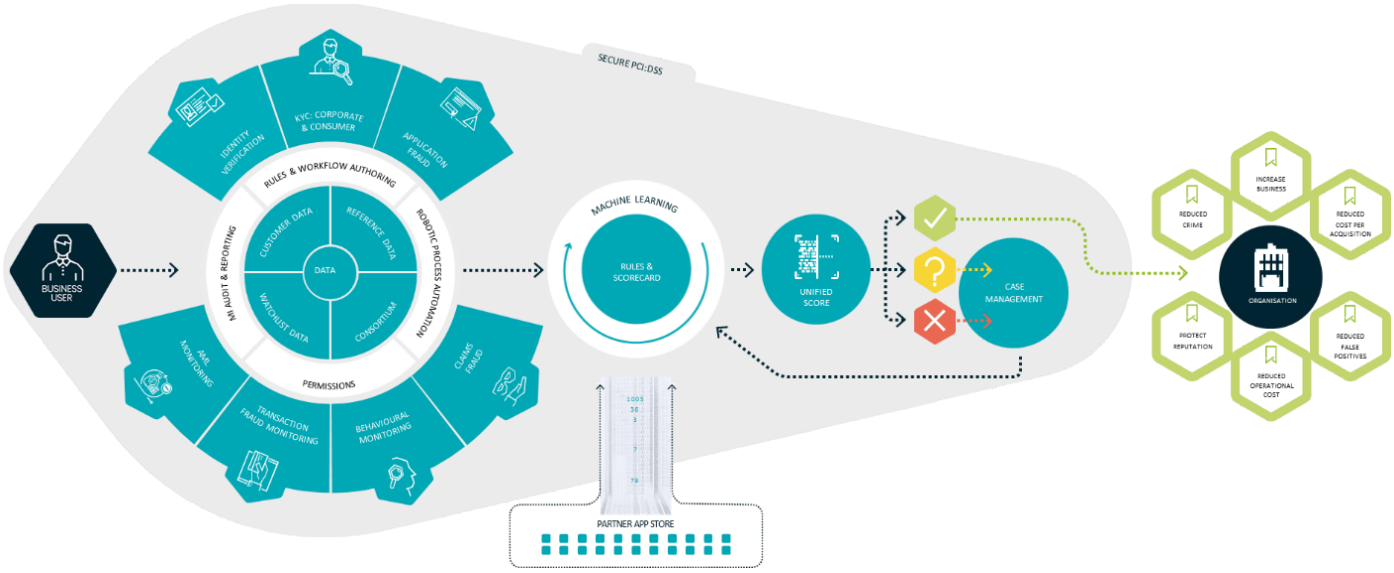
Schedule: Full Solution Overview

Our powerful decision engine sits at the heart of a unified financial crime management process. By managing decisions and scoring data in one flow you no longer need struggle with the complexity and cost of multiple decision points. Insight can be shared seamlessly across identity, fraud and compliance to make decisions with more relevant information in full view. We recognise that modern, digital companies need to be agile and adapt quickly to opportunities and threats. We make this possible by making it easy to spot emerging threats quickly and deploy new strategies implement in minutes. You get a choice of secure cloud or local hosting which is really easy to set-up

The Journeys

The platform is developed by configuration rather than code, therefore allowing the Business User to adapt strategies, write and edit rules, access dynamic reporting management information and integrate new services via our Open API Management platform. To bring this to life we have created a series of pro-compiled Journeys and Apps that are available to use in the Journeys. A journey is made up of workflow, a set of rules, data and third-party services.

- Identity Verification
- Application Fraud
- KYC: Corporate and Consumer
- Transaction Fraud Monitoring
- AML Monitoring
- Behavioural Monitoring



How it Works

Across all of these journeys you are able to benefit from a data Consortium, whereby sharing real-time knowledge and insight increases your chances of on-boarding hero customers, quickly and spotting villains.

The TruNarrative App Store is a marketplace of relevant third party service providers that you can integrate simply into any Journey. With endless apps, ready to use, you can find new suppliers in the app store, or 'bring your own' valued service and integrate in minutes. When these third party services are used in combination with your own data and the data from the consortium this can be truly powerful in enabling you to find more fraud whilst significantly reducing false positives

We use a combination of different analytical techniques, including Machine Learning to enhance scorecards and to optimise your use of rules. By constantly reviewing your outcomes against the rules you use and the rules you don't use, the machine is constantly potting inefficient or ineffective rules and suggesting changes.Even better, if the platform spots a new type of fraud then it can suggest a brand-new rule to combat it, therefore ensuring you adapt to new risks quickly. By then scoring the outcomes from all these insights in one flow and unifying the scoring we remove complexity, increase detection and remove unnecessary cost.

Should the application or transaction pass then an immediate and clear status is returned for straight through processing. If it is flagged as suspect or high risk then it will move into the Case Management area. Through analytics, the case management environment allows you to firstly make intelligent queue processing decisions by prioritising cases by any attribute, including by channel, product and analyst. You see everything you need to make a quick and accurate decisions in this single environment, removing the need to go to other third party tools to investigate. The escalation process and document creation is automated where possible to remove costly manual tasks.

Once a case is investigated, should it be found to be fraudulent or a proven money launderer then this intelligence is shared immediately with your central database so we can identify and flag other potential risks that may be there. Watch-lists are also automatically updated as required.