FinCrime Principles of Inclusion

November 2021

FINTRAIL

Finclusion

FINTECH FINCRIME EXCHANGE

These principles were created in partnership between FINTRAIL and Tech Nation's Fintech Delivery Panel. Please reach out to the authors below for any support or questions around the principles.

Ravi Shukla - Head of FinTech Delivery Panel - Tech Nation
ravishukla@technation.io

Mikey Morton - Senior Consultant - FINTRAIL
michael.morton@fintrail.com

James Nurse - Managing Director - FINTRAIL
james.nurse@fintrail.com

Finclusion Campaign

Finclusion 2021 is a series of connected activities designed to stimulate, inspire, showcase and scale fintech's contribution to financial inclusion – from potential game-changing products and collaborations, to the here-and-now actions being driven by the UK's leading firms reshaping financial services.

As part of the Finclusion Campaign run by Tech Nation's Fintech Delivery Panel, FINTRAIL has collaborated with industry professionals to develop a set of principles for consideration by anti-financial crime professionals.

Use Case

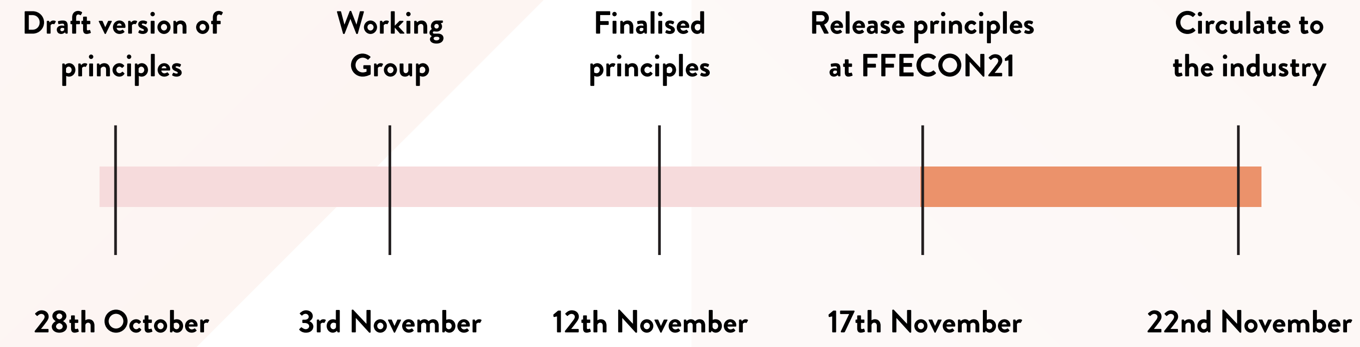
We as anti-financial crime professionals must do more to proactively support financial inclusion and ensure the controls that we design, and how we assure them, do not inadvertently disadvantage those who need access to services the most.

Financial exclusion can affect a variety of different ethnic and social groups. Homelessness, ethnicity, disabilities, and professional status are all factors that can impede access to financial services.

Fincrime Finclusion Principles

These principles are not designed to be used as a checklist but more guiding notes for consideration to enhance financial inclusion in the anti-financial crime world. Businesses are encouraged to consider these principles when:

1. Designing, developing and tuning their anti-financial crime programmes
2. Performing assurance on the effectiveness of their anti-financial crime programmes



Draft version of principles

28th October

Working Group

3rd November

Finalised principles

12th November

Release principles at FFECON21

17th November

Circulate to the industry

22nd November

Principles

Risk Appetite: Your risk appetite as a business should underpin types of activities and services that are above your tolerance level without inadvertently restricting access to financial services to certain groups or categories.

- Does your risk appetite exclude certain groups or categories that may have a harder time accessing financial services (for example, homeless people or asylum seekers)?
- What data are you using to inform your risk appetite, and how credible are your sources?
- Does your risk appetite make preclusive decisions using characteristics protected by jurisdictional laws (for example, the UK Equalities Act)?

Customer Due Diligence: The methods used to conduct customer due diligence should meet your regulatory requirements and help you to assess and understand your risk, but should not create unnecessary barriers to accessing your product.

- Have you conducted testing across your tooling setup to ensure that it does not have the potential to create unnecessary friction for different races or religions? (for example, people with darker skin tones; or who wear a religious garment such as a hijab).
- Do you offer an alternative verification route for people who may find using a selfie photo or video verification method difficult due to a physical or mental disability, or a lack of accesss to technology?
- Do you support the capability for a customer to use a preferred name in conjunction with their legal name?
- Does your customer have the ability to confirm their preferred gender, pronouns, title etc?
- Does your due diligence process ask for proportionate documentation, and allow for alternate routes to verification if the customer does not have standard documentation? For example, a recent immigrant to the UK may only have a British Residency Permit, and not everyone will hold a passport or driving licence.

Customer Risk Assessment: Any customer risk assessment or customer profiling should be based on facts and should not unfairly categorise individuals as higher risk purely based on their gender, age, ethnicity, religion, or social background.

- Do you have risk criteria that may unfairly exclude people from products by categorising them as higher risk based on sweeping profiling e.g. considering every 18-25 year old student higher risk due to the fact they fit certain money mule typologies?
- Do you have risk criteria that automatically assign people a high-risk score based on a single characteristic such as nationality?

Customer Screening: Conscious screening configurations and policies can help ensure that your screening setup does not make product access more difficult for certain categories of customers.

- For adverse media screening, do you have criteria to determine when a conviction becomes irrelevant to the risk the customer presents? For example, using years-old convictions to dictate decisions may make it difficult for past-offenders to get access to financial services. Decisions in this area should also be cognisant of any local laws that mean the customer is not required to disclose the conviction such as the Rehabilitation of Offenders Act in the UK.

- When you make decisions based on adverse media, do you ensure the decision to accept or reject a customer is made in the context of the product the person is attempting to access? For instance, a person with a conviction for being drunk and disorderly does not necessarily pose a heightened financial crime risk.
- Have you configured your screening tooling to not unfairly target certain groups, or make it harder for some customers to pass screening? For example, if you allow Chinese customers to enter their name in Mandarin can your screening handle transliteration and alternate spellings? Is it sensitive to naming conventions, such as the ordering of given names and surnames, or the use of alternative names, middle names or nicknames on formal documentation?
- Does your screening contain any blanket ban rules around names such as "Islam"?

Enterprise Wide Risk Assessment: This assessment creates a financial crime risk overview that helps determine all of your controls, procedures, and policies. It's important that the risks are collected and assessed in an objective manner free from bias or prejudice.

- How do you ensure your highlighted risks are justified and do not discriminate against certain groups or individuals?
- Do you associate the colour black with negative or critical risk areas? Could you use another colour to indicate this?

Transaction Monitoring: As you monitor and make decisions based on customer behaviours, it is important that your analysts and alert handlers are trained to be aware of unconscious and internal bias that may lead to unfair customer outcomes.

- Can your analysts view KYC information in conjunction with the alert and do you have any concerns this may create a biased outcome? Can you consider how the information is presented, such as concealing the ID photograph or customer name, or presenting the alert information for review first before clicking through to the KYC information?
- How do you train your machine learning and artificial intelligence engines? Are you confident that they are not operating within any discriminatory parameters? Additionally, how often do you review those models post initial training and deployment?
- How do you treat higher risk jurisdictions and the persons transacting with them? Do you consider them default high risk, or do you look deeper to understand the actual risk posed?
- Do you regularly assure and update your watchlists to ensure they're current and do not include outdated entries that may cause exclusion?

Investigations: It's crucial that investigators understand the differences between typologies and stereotyping to avoid letting unconscious or pre-existing bias guide their decisions.

- Does your investigation team understand how to use profiling in a non-discriminatory way during investigations? For example, not making decisions based on a single factor but triangulating concerns with other findings / context to draw a conclusion.
- Do you provide your team with training to understand bias and how to recognise it when conducting investigations or case profiling?

Training: Training programmes that include inclusivity across all topic areas work to ensure you are really underpinning your financial crime frameworks and programmes with inclusive thinking and processes.

- How do you consider inclusivity when desigining or developing your complaince training programs?
- Has your team received vulnerable customer training so they're able to identify signs of vulnerability? This is particularly key in recognising the differences between vulnerability and financial crime. For example, could your analyst identify where someone may be being victimised rather than facilitating financial crime?

Policy: This is where you set the tone for your financial crime programme. Inclusivity should be considered when making any policy decision, and inclusive language used throughout any written policy document.

- Do you use inclusive language in policy and procedures documentation?
- Do you have policy documentation that clearly states that behaviours that promote hate, discrimination, racism, or violence will not be tolerated on your platform?

Hiring: Diversity and inclusion should naturally be at the core of all your hiring plans, however it's especially important to ensure that you hire a diverse pool of candidates into decision-making roles to really reap the benefit of people's varied experiences and background.

- Are you hiring a diverse group of anti-financial crime professionals who can contribute to more rounded opinions on risk perception and mitigation?
- Do you ensure you have a diverse representation of people at all levels in your organisation, including leaders and decision makers?
- Do you have forums that enable diverse groups of people to contribute and influence decisions, ensuring that a variety of opinions based on different experiences can be heard?
- Do you have resources available to your hiring teams to ensure they understand the importance of diversity, equality and inclusion ("DE&I") and how to handle it in a hiring context?

Regulatory Change: Anti-financial crime regulations continue to change with the threat landscape and regulators should also ensure that inclusivity is considered in their development.

- Where opportunity arises, participate in any consultations to ensure inclusivity is a core consideration and do not be afraid to challenge the regulators.
- When interpreting regulations, consider how they can be applied inclusively and where you identify areas that cause exclusion, raise it to your regulators.

Measuring Effectiveness: Continually monitoring your programme against DE&I metrics is key to ensuring it is operating as you'd expect and is not just a hollow policy statement:

- Do you view your management information from an inclusivity lens; for example, interrogating whether a certain piece of data or information is influenced by an issue with inclusion?
- How many people belonging to under-represented backgrounds go though more than one attempt to clear your identification verification processes?
- How many people belonging to under-represented backgrounds are off-boarded / blocked, with the decisions then revered upon appeal?
- How many people use your product from marginalised communities, and do you understand the reasons behind that data?
- How many people from under-represented backgrounds have you hored into FinCrime leadership roles?

Thank You

v1 - November 2021

FINTRAIL

Finclusion

FINTECH FINCRIME EXCHANGE