Disrupting Financial Crime

Best Practice in Customer Due Diligence Among Fintechs

White Paper

by the

FinTech Financial Crime Exchange

May 2017

FINTRAIL

RUSI
www.rusi.org

Abstract

Financial technology companies (fintechs) leverage online and mobile applications to offer new financial services with efficient and cost-effective customer experience. However, the non-face-to-face (non-f2f) nature of fintech businesses poses risks that fraudsters or other criminals may seek to exploit these remote platforms and related products.

Robust customer due diligence (CDD) is one element of an overall risk management architecture that can mitigate these threats. Fintechs are uniquely suited to harness and develop innovative CDD approaches, owing to their dynamic business models and comfort in using technological solutions.

This white paper describes examples of best practice in CDD among members of the FinTech Financial Crime Exchange (FFE), offering practical insight for fintech companies and other stakeholders – such as banks and regulators – seeking to better understand the industry. It provides examples of how fintechs are utilising innovative CDD approaches to manage risks while also enabling a high-quality customer experience. For example:

- Fintechs are leveraging numerous data points and employing innovative analytical approaches to enable a dynamic and holistic view of customer risk.
- This includes the use of facial recognition techniques, interactive user interfaces, innovative document scanning and analysis, Internet Protocol (IP) geolocation, predictive analytics and machine learning.
- These solutions can enable fintechs to employ a genuinely risk-based approach to CDD as their customer base and service offerings evolve.

This paper also assesses areas where fintechs can benefit from further development and exploration. For example:

- Fintechs should carefully consider the appropriate balance of in-house and third party solutions for their business model.
- Fintechs must be prepared to conduct thorough and formal assurance testing of both in-house and third-party solutions and outsourced services.
- As they scale, it is important that fintechs have in place adequate governance arrangements to manage risks that come with changes to their CDD systems and controls.

About the FFE

The FFE was established in January 2017 as an intra-industry partnership. It promotes an increased understanding of financial crime by the fintech industry. It provides a collaborative forum for fintechs to discuss financial crime typologies, risk management approaches and regulatory challenges. Its objective is to inform, debate and develop knowledge and best practices. Its members meet monthly to discuss these topics. As of May 2017, the FFE includes 17 participating members from the UK fintech industry. Its meetings are hosted by the Centre for Financial Crime and Security Studies at the Royal United Services Institute (RUSI), a British think tank, and are organised in coordination with FINTRAIL, a UK financial crime risk management company.

Enquiries about the FFE can be directed to the FFE Secretariat. For further information please contact Rebecca Marriott (rebecca.marriott@fintrail.co.uk) or Florence Keen (florencek@rusi.org).

Companies that are among the members of the FFE include:

Curve

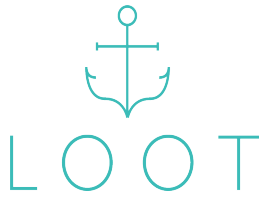


Table of Contents

Introduction

Fintechs provide customers with new financial products and services as an alternative to the traditional offerings of incumbent financial institutions. Mobile pre-paid services, mobile current accounts, peer-to-peer lending and e-invoicing services are just several among the range of offerings fintechs provide their customers. Fintechs also feature a new model of customer experience that disrupts traditional financial services approaches.

- Fintechs generally rely on exclusively non-face-to-face (non-f2f) business to provide their customers with efficient and cost-effective services.
- Fintechs leverage online and mobile technology, and harness related data, as a central component of their operations, and not merely as an extra or incidental feature, as in the case of incumbent financial institutions.
- Fintechs are unencumbered by extensive branch networks and other costly physical infrastructure. This allows them to address the requirements of a modern customer base and to provide dynamic service offerings.

Despite these advantages, fintechs' non-f2f business models present financial crime risks.

- Fraudsters, money launderers, sanctions evaders and other criminals may attempt to access fintech services for both the degree of remote interaction they offer, and the relative speed with which new customer accounts can be created.
- Start-up companies are especially vulnerable. Criminals may target young firms and their new products, seeking to exploit weaknesses in immature control frameworks.

Robust customer due diligence (CDD) practices are critical to mitigating these risks. This white paper sets out examples of best practice in CDD among fintechs, based on the experiences of members of the FFE.

Because of their innovative use of technology, fintechs can readily adapt and employ new, sophisticated approaches to the design and deployment of CDD.

- Facial recognition, innovative document scanning and analysis, IP geolocation, predictive analytics and machine learning are among the solutions fintechs are employing in their CDD processes from early on in their development to form a dynamic and holistic view of customer risk.
- High-quality and high-tech CDD, both at customer onboarding and throughout the customer lifecycle, can ensure that non-f2f business is conducted to successfully detect and deter the most significant risks without undue negative impact on the experience of legitimate customers.
- FFE members treat transaction monitoring as an integral component of CDD, scrutinising customers' ongoing activity and behavioural patterns and factoring them in as risk indicators.

This enables a more complete view of customer risk than if CDD and transaction monitoring are highly segregated functions. The use of techniques such as machine learning, predictive analytics and data mining can facilitate a dynamic view of customer risk based on ongoing activity.

- Fintech start-ups have an advantage in this regard over incumbent financial institutions: where incumbents must retrofit new technological solutions on long-established systems and customer bases, fintechs can integrate these innovations into their operations from the outset, enabling a dynamic, risk-based approach to CDD as their customer base and service offerings evolve.

Fintechs' often relatively small size and start-up status also pose several operational challenges and risks. It is important that fintechs consider how to address these.

- Because of their expertise in tech development and data analysis, fintechs are well-positioned to develop innovative in-house CDD solutions and tools; however, in-house solutions must still be regulatory compliant and should be subject to meaningful governance and assurance processes. Fintechs should also carefully consider the appropriate balance of in-house and third party solutions for their business model.
- Some fintechs are heavily reliant on third party providers for CDD-related services, such as transaction monitoring and sanctions and PEP screening. This exposes fintechs to potential risks if those third-party services are inadequate. Fintechs must be prepared to conduct thorough and formal assurance testing of third-party solutions and outsourced services.
- Smaller, newer fintechs may benefit from having flexible or less structured processes for instituting changes in their control framework, including changes to CDD policies and procedures, than might be typical at an incumbent financial institution. However, as they scale, it is important that fintechs have in place adequate governance arrangements to manage risks that come with changes to CDD systems and controls.

This white paper discusses these and related issues in detail.

Methodology

The FFE Secretariat drafted this white paper in April 2017 at the request of the FFE's membership. The Secretariat circulated questionnaires among the FFE's members to obtain information about the CDD processes and systems they rely on, and to understand challenges they face in establishing and operating those processes and systems. In addition to the written feedback it received from members, the conducted additional phone interviews with several members to provide more detailed consideration of CDD practices and related topics. Examples of solutions and related typologies were also drawn from ongoing meetings among FFE members, and from a risk assessment exercise the FFE Secretariat conducted in February 2017.

Because the FFE's membership includes a broad range of fintechs – including challenger banks, international payments companies, student payment services, pre-paid card providers, service aggregators, peer-to-peer (P2P) lenders, e-invoicing services and others – the Secretariat believes this white paper offers a meaningful high-level view into the issues faced broadly among fintechs. Because most of the FFE members participating in the survey serve personal retail customers, the examples given here are generally retail-focused. However, certain core principles – such as the importance of a risk-based approach, the advantage of maintaining a dynamic view of customer risk, and the need for robust governance and assurance arrangements around controls –apply to business customers as well, and the paper contains some examples of practices that FFE members serving business customers utilise.

This white paper is for use by the FFE's membership and Secretariat to facilitate ongoing discussion among the group. It will also inform discussions with external stakeholders, such as regulatory agencies and industry bodies.

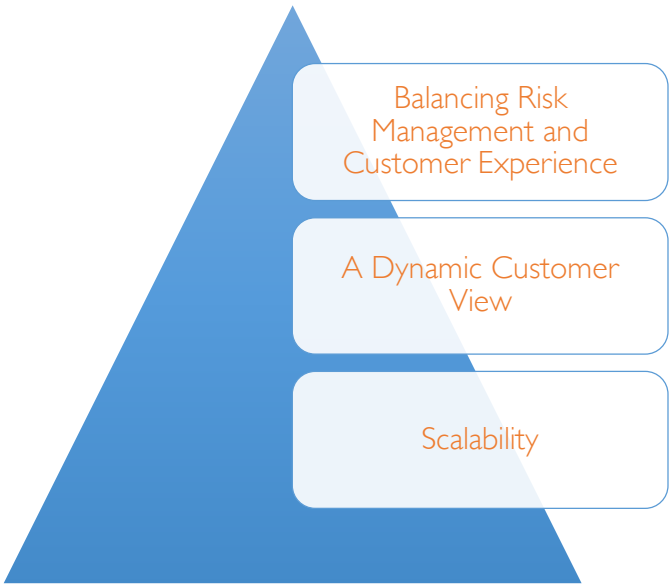
Fintechs and CDD: Elements of Best Practice

As observed among FFE members, best practice in CDD among fintechs incorporates three general components:

- achieving an appropriate **balance** between robust risk management and a high-quality customer experience;
- obtaining a **dynamic** view of customer risk drawn from numerous data points; and
- deploying a **scalable** approach that can evolve as a fintech company grows.

These are described in further detail below.

Foundations of best practice in CDD among fintechs



Balancing Robust Risk Management with High Quality Customer Experience

Fintechs derive a competitive advantage from their non-f2f business models, which can also benefit consumers: speedier on-boarding and remote interaction reduce costs for fintechs while providing a less cumbersome process for customers than they would tend to encounter at an incumbent financial institution.

However, UK regulators and industry groups have been clear on the risks that arise in non-f2f business. The UK Money Laundering regulations set out requirements for firms to take risk-sensitive

measures towards customers who are not identified in person.[1] The Joint Money Laundering Steering Group (JMLSG) cites the remoteness, ease and speed of online business as a heightened risk factor for money laundering purposes.

Among fintechs, best practice in CDD ensures that the customer's experience is not degraded, while also enabling the effective and proportionate detection and mitigation of risk.

Examples of best practice that enable FFE members to achieve this balance when onboarding their customers include:

- Streamlined but robust applications for identification and verification (ID&V). In addition to applying basic ID&V measures as required by the UK Money Laundering Regulations – such as checking a prospective customer's name against electoral roles and requiring an initial deposit from an existing UK bank account – FFE members employ other solutions for ensuring that customers, and the documents they supply, are genuine.

    - Document scanning and validation: FFE members employ solutions to enable their customers to use mobile phones, laptops, tablets and other devices to photograph or scan images of documents that are transmitted directly to the company, typically via the company's own app. This has the advantage of creating ease for customers, while mitigating data protection risks that might come with customers sending documents via unencrypted email or other unsecure methods. For personal retail customers, this will generally include a passport or other form of official photo ID. In the case of business customers, this can include corporate registration documents. Many scanning solutions can validate documents rapidly, sometimes in a matter of minutes, extracting data which can highlight possible fraud and misrepresentation, while enabling rapid customer onboarding. The most effective of these solutions can successfully recognise and validate the authenticity of numerous forms of ID (passports, driving licences, residency cards, etc.) from numerous countries.

      In addition to ID verification, some FFE members use document scanning and uploading for address verification. This can include scanning or uploading of utility bills, pay slips, tax forms and other documentation. One member noted that when

[1] Regulation 14(2) of the Money Laundering Regulations 2007 sets out that, "Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures –

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution."

they disburse a prepaid card, the customer must receive it at the address from which they applied and then must scan an image of the card into the company's app; this confirms the receipt of the card, and helps to validate the customer's address information simultaneously.

Some FFE members also indicated that they apply similar validation techniques to those noted above when obtaining documents, such as pay slips, related to source of wealth information for politically exposed persons (PEPs) and other high risk customers.

One FFE member said their company reviews metadata from documents to evaluate authenticity. This includes analysing GPS location data embedded in ID documents against a customer's residential address and collected IP information to determine whether the documents are authentic. The same company also analyses the image compression of documents: if different parts of an image are compressed at different levels, that suggests a document may have been manipulated, for example via Photoshop.

- Interactive interfaces for additional validation: In addition to scrutinising customer documents, several FFE members surveyed use interactive interfaces to verify customers' existence. In most cases this involves the customer using the company's app to photograph themselves, which the company can then assess against the customer's ID documentation. Often this includes software that recognises facial movement when the photo is being taken to ensure authenticity. In addition to requiring customers to take a photograph, one FFE member surveyed requires customers to use the company's app to record a video of themselves speaking a specific sentence.

  Not all FFE members require every customer to undertake photographic or other facial recognition verification where customers' identity can be validated through other means – such as when UK customers can be verified via automated matches against electoral roles and through e-KYC platforms. However, one company that exempts app-based photographic verification in certain instances said it will still conduct photographic verification methods on a risk-sensitive basis. For example, customers who fail e-KYC, are higher risk or that operate above certain monetary

thresholds may be required to undergo photographic validation using app-based software.

Beyond facial recognition analysis, FFE members surveyed do not rely on extensive biometrics – such as fingerprinting or iris scanning – at present, though some indicated they are exploring how they might increase their use of advanced biometrics in the future.

-  Online behaviour analysis: FFE members indicate that they use a variety of data points to analyse prospective customers' online behaviour that may provide indicators of fraud or other financial crime risks at onboarding. This can include: conducting risk analysis around a customer's email address (for example, to determine whether it was newly generated solely for the purposes of opening the account, whether it was created in a high risk jurisdiction, or has been reported by other merchants as associated with fraud); analysing whether text may have been copied and pasted into an online application form (for example, by fraudsters attempting to make numerous applications); and observing the time taken to navigate websites or complete an application (for example, fraudsters may go through an application process very quickly, using information already generated from other fraudulent applications). One company surveyed indicated that in addition to using third party service providers to assess potential fraud risk at onboarding they use an in-house logic system to assess for fraud risks based on a customer's online application.

- An appropriate, risk-based balance between manual and automated verification. All FFE members surveyed engage in a combination of manual and automated verification of gathered information. Most members will initially direct customers to use automated verification methods, but if those fail – for example, owing to a failed document scan or a lack of matches against electoral rolls – the company will verify documents manually. One member stated that they will request certified copies of documents where automated checks produce no results. Importantly, members do not exclusively rely on automated verification, but seek to use both manual and automated verification on a risk-sensitive basis.

  Combining manual and automated verification methods mitigates against both the risks of human and machine error while ensuring a more robust set of controls than exclusive reliance on either method. Where there are questions about documentation or information that require clarification from the customer, FFE members will generally resolve these by in-app or online chat support, or by phone. This mobile interaction with clients enables both good practice in CDD and a more frictionless customer experience, and may present an advantage

over the approach of some incumbent financial institutions, which in certain cases may still communicate with clients primarily by post to obtain information, risking a non-response.

- **Aiming for a frictionless customer experience while remaining compliant.** One risk fintechs face is over-emphasising a rapid customer onboarding process at the expense of robust compliance procedures. This requires obtaining certain basic information about a prospective customer to enable a risk-based view of whether an account should be opened or card or other product issued. All members surveyed conduct sanctions and PEP screening at onboarding and throughout the customer relationship as one component of determining suitability. One FFE member that provides pre-paid card services said that in addition to PEP, sanctions and adverse media screening, their account opening process includes ID checks, an analysis of fraud indicators using a third-party provider, and the application of an in-house logic system to detect risks; the results from this process determine whether and what services to offer a customer before any card is issued.

  Some members note that to date they have offered a small range of products with strict transaction limits using simplified due diligence (SDD). However, some indicate they may generally move away from SDD with impending changes to the UK Money Laundering Regulations and the European Union's Fourth Anti-Money Laundering Directive, and will likely use a binary approach of performing either standard CDD or EDD.

A Dynamic Customer View

A key distinction between fintechs and many incumbent financial institutions involves the way customer risk is determined and monitored. Many incumbent financial institutions operate with a largely static view of customer risk, as demonstrated in Figure 1 below, that places heavy reliance on information gathered at onboarding.

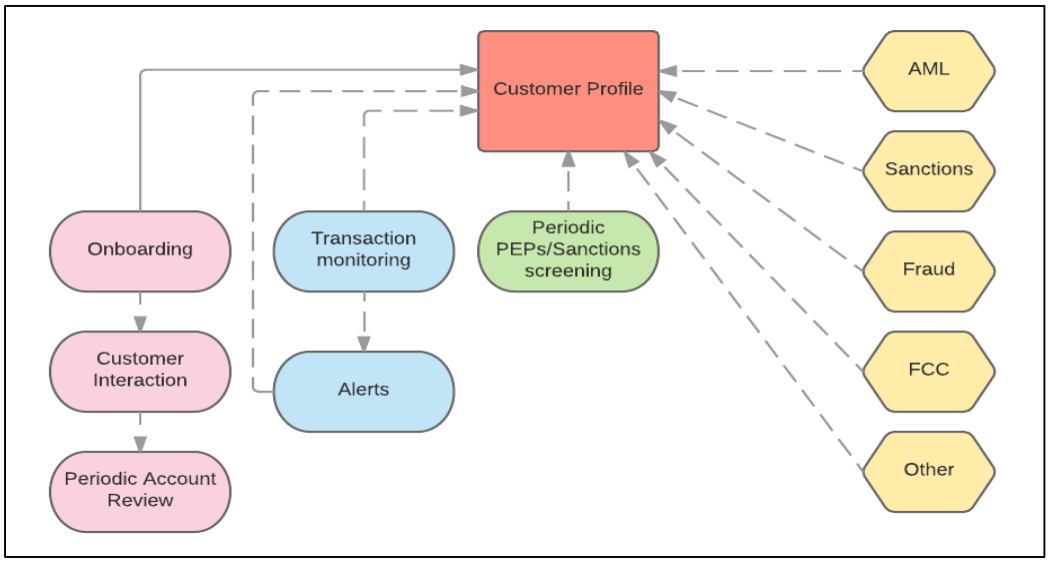


Figure 1 above represents a traditional approach to customer risk management, often employed by incumbent financial institutions. Initial information is gathered at onboarding to establish a customer risk rating. Other aspects of monitoring – such as transaction monitoring, activity alerts, and periodic review – may be incorporated into the customer risk rating, though whether this occurs depends on whether the firm's processes and internal review teams are linked. (Dashed lines represent processes that are at risk of not being factored in as part of the customer risk assessment). Numerous, sometimes fragmented, internal teams with specialised functions for monitoring types of financial crime – such as AML, Sanctions, Fraud and general Financial Crime Compliance (FCC) – may or may not refer to this information, depending on the nature of the customer's activity. Similarly, ongoing investigations carried out by these segregated teams may not always have an impact on the customer's risk rating.

This approach focuses on gathering large amounts of information about a customer up front, which can offer an advantage to risk-averse financial institutions. However, this approach comes with its own risks. As Figure 1 indicates, traditional CDD methods are often heavily siloed and fragmented; information about customers is obtained on an ad hoc basis, and in certain cases some information – such as transaction monitoring information – may not be factored into the view of customer risk. These approaches often may rely on outdated data disbursed across numerous unintegrated systems.

Surveys of FFE members suggest that they take a more dynamic approach to assessing and managing customer risk, as demonstrated in Figure 2 on the next page, that is suited to their often-unconventional operating models and product offerings. In surveys and interviews, FFE members described a range of specific, idiosyncratic approaches they take to CDD; however, all attempt to employ an iterative risk assessment process that leverages numerous data points on an ongoing basis throughout the customer lifecycle to enable a complete and up-to-date view of risk.

Several FFE members indicated that they have a formal and structured customer risk scoring methodology that places customers into clear risk-based tiers of High, Medium and Low risk. Others indicated that a heavily structured customer risk scoring approach is generally not suited for their business model, and instead, they rely on a variety of data points, and anomaly detection, to provide an indication of customer risk over time.

One FFE member indicated that very early in its history it used a three-tiered customer risk scoring method at customer onboarding, but changed their approach after determining that it wasn't suitable for a company providing a limited range of retail products across limited geographies. This company, like several other FFE members surveyed, now only risk rates customers at onboarding as either neutral or as high-risk (for example, where the customer is a PEP, or if the customer seeks to engage in transactions above a certain pre-defined monetary threshold). It is after the customer begins account activity that these companies attempt to acquire a more complete picture of customer risk – methods of which are discussed in further detail below.

However, some FFE members use a more structured counterparty risk rating method at onboarding. For example, one member described that it will soon deploy a three-tiered (High, Medium, Low) customer risk scoring model where customers who fall outside the company's general target age demographic and who would generally have less reason to use the product will be classified at minimum as Medium risk by default, and where PEPs and certain other customers will be rated as

High risk. The company's typical target customer base will generally be rated as low risk, except where specific risk indicators of greater risk are present on a case-by-case basis.

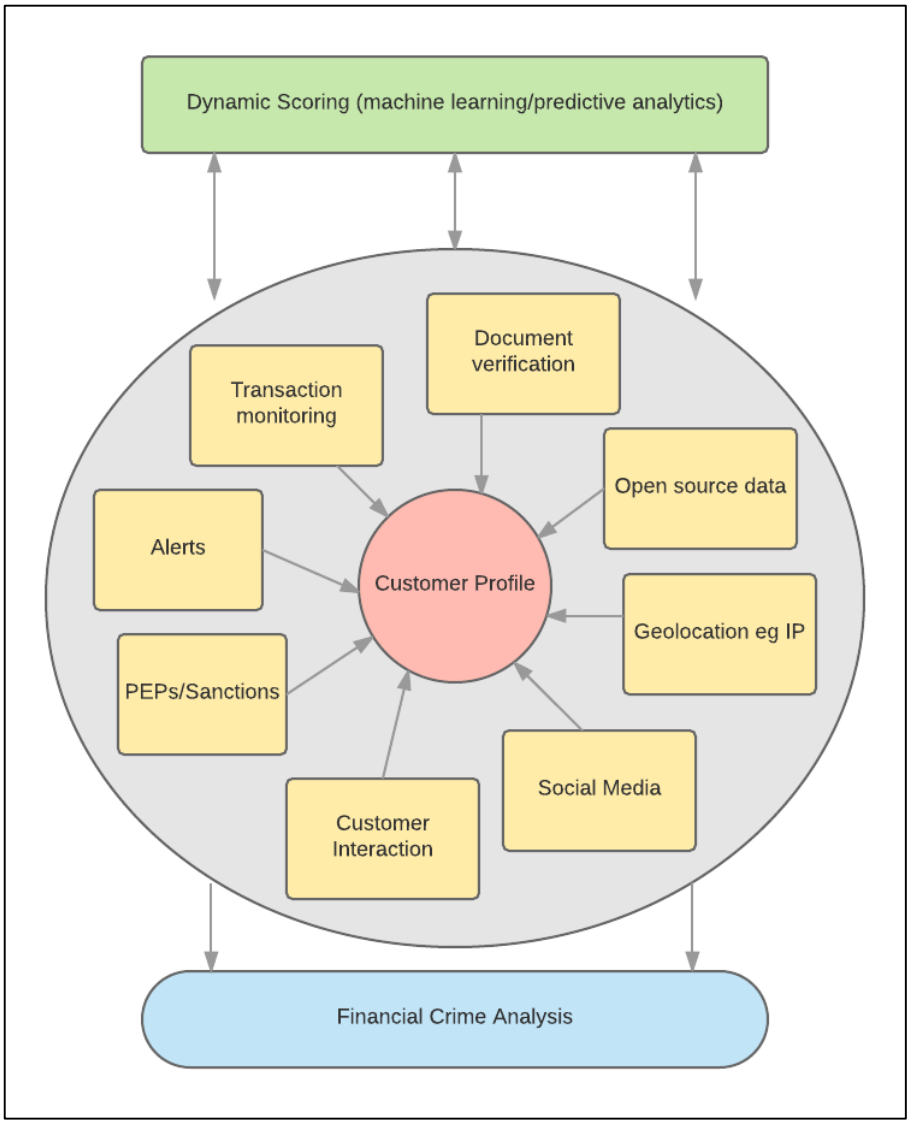


Figure 2 above represents a general target customer risk management model among fintechs. Unlike the traditional model in Figure 1, this approach seeks an iterative process of assessing customer risk. A wide variety of data points are used to provide an ongoing, real-time assessment; this presents opportunities for a dynamic customer risk view, which can be augmented using machine learning or predictive analytics. This provides Financial Crime Compliance teams with a holistic view of customer risk.

What each of these approaches has in common is the need for a careful risk-based consideration of a company's business model, customer base and product offerings to determine the most appropriate and effective approach for assessing customer risk at the outset of a relationship. (Members surveyed indicated that prospective customers who appear on sanctions lists will be denied an account.)

Whether they use a structured risk rating approach at onboarding, all FFE members demonstrate another commonality: for purposes of ongoing CDD, after a customer has been onboarded, they take a dynamic view of customer risk by harnessing and integrating an array of data, which allows them to adjust their view of risk in real-time as the customer's behaviour evolves.

Rather than attempting to form a complete view of customer risk up-front – an often-impractical task – FFE members, after making an initial assessment, allow the customer's activity and other known information to drive the view of risk over time, and for CDD requirements to adjust with that picture. Unlike many traditional incumbent financial institutions, which may only update CDD information at times of periodic review, or on occasion based on certain "trigger events", FFE members surveyed work to obtain a constantly evolving view of customer risk.

As one FFE member described their approach, rather than basing their view of a customer's geographic risk purely on static information – such as the customer's registered address or stated place of business, an approach commonly taken by incumbent financial institutions —the company "use a combination of IP activity and countries from which funds originating from and/or are going to." This approach allows this FFE member to obtain a view of genuine customer geographical risk that is based on observed rather than merely declared activity and that in their view is more sophisticated than traditional approaches.

Harnessing Data

Obtaining a dynamic view of customer risk involves utilising numerous data sources. As the FFE member that works to obtain a dynamic view of geographic risks described it, "data points are gathered about customers rather than from them." This contrasts with the traditional approach of many incumbent financial institutions, which may rely largely on statements or information provided directly by customers at onboarding, with only occasional reference to transactional details or open source searches to understand how customer risks are evolving.

Examples of data sources FFE members routinely utilise for ongoing monitoring purposes include:

IP geolocation: All FFE members surveyed indicate that customer IP addresses provide an important data point for determining customer risk levels and detecting anomalies in behaviour. As mentioned above, one FFE member uses IP addresses as a factor in determining customers' geographic risk. Logins to the company's app or website from higher risk jurisdictions can be a factor in elevating the customer's risk rating. Other members stated that IP addresses provide a critical data point in activity and transaction monitoring, enabling them to identify inconsistencies in behaviour that can form a basis for further investigation.

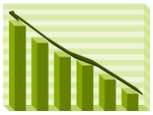
Device monitoring and blacklisting: Some FFE members also rely on device monitoring to assess customer risk. Information about mobile devices enables them to detect anomalies or activity

of concern. For example, if a customer account has been terminated due to concerns about fraud but then attempts to open an account under a different name but using the same mobile device, monitoring can detect this behaviour.

Social media analysis: Some FFE members also look closely to social media sites – such as Facebook, LinkedIn and Twitter – to gather additional information on customers or related parties. Social media analysis requires scrutiny of the reliability and validity of information, but can provide a useful source for fintechs where they exercise caution in evaluating the reliability of that data. For example, one FFE member said that where they require customers to provide information on source of wealth, in addition to providing information such as a pay slip, the customer can connect their LinkedIn profile to their profile in the company's app; this allows the company to consider whether information the customer provided is consistent with information they publish about themselves publically, and to monitor for changes in the customer's behaviour based on their evolving public profile.

Harnessing commercial and credit data: FFE members generally emphasised that any data point can inform their view of customer risk. This includes commercial information or credit data they may obtain through their general interactions with customers. One FFE member that provides services to business customers says it conducts automated monitoring of Companies House entries so that changes among a customer's owners or directors will prompt requests for updated CDD information. Fintechs often market their product offerings to very specific demographics; therefore, if compliance staff understand the company's target demographics and product offerings, they can better evaluate whether any new customers and their activity fall outside the identified norm.

Direct customer interaction: Some FFE members indicated that while they look to numerous data points in developing a customer risk picture, direct human interaction remains an important component in assessing customer risk. Service and support teams that contact customers by phone or email, or by in-app messaging support, can obtain information about customers and provide an indication of possible risks that would otherwise go undetected. One FFE member that provides services to business customers noted that it has dedicated account managers are responsible for conducting AML/CTF checks, and that dedicated onboarding staff maintain ongoing interaction with customers throughout the onboarding process.



Automated transaction monitoring: All FFE members indicated that automated transaction monitoring is a critical component of how they assess customer risk– though the way this occurs varies significantly based on their business models. One company indicated that it undertakes ongoing general data mining in addition to scrutinising alerts flagged by automated systems. A key factor in the success of transaction monitoring systems is the ability to customise rules and thresholds, regardless of whether the company uses an in-house transaction monitoring system, or a solution developed by a third-party provider. Members also noted that they employ a risk-based approach to transaction monitoring, applying different levels of scrutiny and due diligence to certain types of transactions, products and value thresholds.

FFE members look to transaction monitoring as a critical component of CDD. This distinguishes them from many incumbent financial institutions, which may treat CDD and transaction monitoring as highly segregated functions. The traditional approach poses an operational problem: changes in customer behaviour and transaction activity may not always be factored into the view of customer risk; this can create a situation where a firm applies inappropriate levels of CDD to a customer engaged in high risk activity. FFE members, on the other hand, harness live transactional information as a component of customer risk to ensure customer risk scoring is updated in real-time and ensures they apply a level of CDD commensurate to risk inherent in the customer's ongoing activity.

Machine learning/predictive analytics: Many FFE members indicated that they employ innovative automated techniques to assess information and form a dynamic view of customer behaviour. This includes machine learning in transaction monitoring tools, and the use of predictive analytics to obtain a view of risk in behavioural patterns.

What FFE members say

"We believe that machine learning is a valuable tool that we continually invest in that will allow us to have effective, efficient, and sustainable coverage as we scale."

"[Our] transaction monitoring system incorporates machine learning, and the customer risk rating is constantly factoring in customers' activity to increase/ decrease their rating."

The use of automated solutions that enable a dynamic view of customer risk and detect anomalies in behaviour offers several benefits to fintechs.

First, they reduce the level and intensity of manual labour required for certain tasks, enabling staff to focus on critical decision-making and contextual analysis about customer activity.

Second, utilising automated and ongoing data collection and dynamic risk scoring reduces the likelihood of failing to capture data or information requested from a customer solely on an ad hoc or periodic basis.

Third, automated solutions are often able to identify patterns or anomalies in behaviour that a human would not, particularly among large data sets.

Finally, a dynamic risk scoring approach enables a holistic view of customer risk. Rather than seeking to capture information purely from the standpoint of money laundering, fraud or other specific risks in isolation, some FFE members indicated that they constantly attempt to obtain a complete view of the range of financial crime risks a customer may pose.

Scalability

Because fintechs often rapidly evolve in size and product offerings, it is important that their CDD approaches are scalable. Fintech start-ups must prepare to have CDD processes and policies they can implement from the moment they launch, but should not assume that the initial process they implement will last. Similarly, larger companies must be prepared to regularly review the adequacy of their established systems and controls. FFE members surveyed are giving careful consideration to these issues. However, this remains an area of potential operational risk generally across the industry. There are several key considerations for fintechs as they scale:

- **In-house vs. third-party services:** Fintechs face a decision about whether to develop their own systems and controls, or whether to utilise third party services or outsourcing arrangements for certain CDD functions. FFE members generally maintain a balance, utilising some third-party services while developing other compliance tools in-house – though some favour one approach more strongly over another. Whether and how they do so is specific to the scale and nature of each company's business. The determination about whether to continue with third party or in-house tools is one that may evolve as a company scales. Such decisions should be made carefully, using a risk-based approach, and with reference to the company's risk profile and risk appetite. One company stated that "in-house tools are built in such a way that allow us to adjust rules and thresholds in real time and as needed according to our risk assessment." Both in-house and outsourced solutions should be subject to regular and rigorous testing, and the rationale for their design and utilisation should be clearly documented.

- **Governance:** As a fintech grows, it should consider how it institutes control changes, such as the implementation of new screening and monitoring tools, or the adjustment of rules and thresholds. Smaller companies that are rapidly expanding may benefit from a nimble and less structured approach, while larger companies may require a more structured set of governance arrangements – though the nature of these arrangements may vary widely based on a company's business model and risk profile.

Among FFE members, most have a designated individual – such as the head of compliance or money laundering reporting officer (MLRO) – who carries out this function. One member indicated their company's intention to form a risk committee that can draw on management information to review and approve changes to controls as the company expands its services. The development of adequate financial crime governance arrangements remains an area for further exploration and industry discussion.

- Suitability of tools: Fintechs should resist the temptation to implement novel or complex CDD solutions for their own sake. As one FFE member noted, "you should think about what tools you need to solve a problem," and not just attempt to adopt new high-tech approaches where others will do. Controls should not be designed or implemented without a clear understanding of their purpose. It is important that companies consider whether certain controls are required, and if so, to document the rationale for their design. For example, the same member said that their company has not instituted machine learning in transaction monitoring as they have felt to date that it would offer little benefit; instead, they have used predictive analytics to detect anomalies in customer behaviour. As the company grows, they are examining the utility of deploying machine learning. Another member indicated that they have opted not to use app-based facial recognition techniques and feel that manual verification is more suitable to their risk-based approach.

- Formalising processes: A fintech's size, scope, nature of business and planned expansion will generally determine how formalised certain compliance processes are. For example, some FFE members have a formal end-to-end process for exiting customer relationships based on financial crime compliance concerns, setting out specific circumstances under which customers should accounts should be terminated. Other members, however, given factors such as their size and product offerings, have found that a less structured, case-by-case approach to making customer termination decisions is more appropriate, though this could change as they scale. As one member described it, as their company grows, they "are looking to ensure all exit scenarios are covered to avoid confusion when a new situation presents itself."

  Such considerations should go together with the development of governance arrangements noted above. The nature of these process and arrangements will vary significantly from company to company but should be developed using a risk-based approach.

CDD in Action: Disrupting Financial Crime

When applied successfully and comprehensively, the CDD best practices described above can have an immediate impact in disrupting illicit behaviour. During its initial meetings, the FFE has identified several financial crime risks that are prevalent among its members. For example:

- First party fraud: Prospective or existing customers may seek to obtain services fraudulently and exploit fintech products via misrepresentation. This may include the use of false documentation or stolen details. P2P lending products and pre-paid card services are particularly vulnerable to first party fraud.

    - A common typology FFE members have noted is use of stolen card details to attempt to load a balance on a prepaid card that is in the customer's name. Payment monitoring using tailored rules can enable detection of this risk.

Case Study – ATM Reversals

One FFE member described a typology of a gang of customers committing ATM reversal fraud. This is where the ATM is tricked into thinking the customer has not taken the money from the ATM, and reverses the transaction, when in fact they have withdrawn the funds. In this instance, the customer would load the card with £250-260 by Faster Payments, and overnight commit the ATM reversal for £250 (the ATM limit) before emptying the account. The gang was connected via shared surnames, addresses and postcodes, and nationality. The gang was identified via transaction monitoring and the use of efficient rules, and with reference to onboarding documentation and other known customer data.

- Third party fraud: Fraudsters may also attempt to open applications in the name of another individual. To date, FFE members suggest they encounter fewer instances of third party fraud than first party fraud, largely owing to the strength of ID&V controls and account activation solutions that can prevent third party fraud; however, companies providing P2P lending and card services may be more vulnerable to this activity.

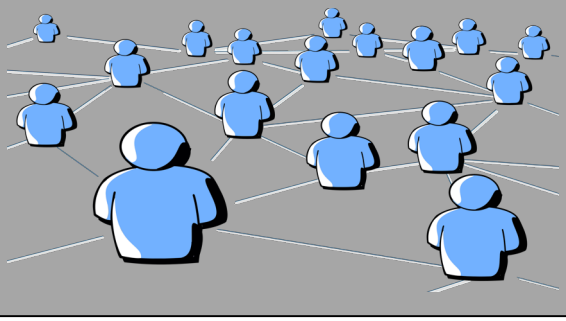
    - FFE members have noted instances where photographs or video taken via their app did not match the photos on ID documents. These companies have denied account opening in such instances.

- Money laundering: Criminals may seek fintech services for their ease of use for purposes such as "smurfing" or money mule activity. Individuals working for criminal networks may attempt to open numerous accounts at a single fintech for these purposes, looking to take advantage of speedy on-boarding times. Fintechs that offer prepaid card services and international payments are particularly vulnerable to money laundering risks, though these may be mitigated in part through transaction limits. Companies that offer business accounts with high turnover are likely to face greater money laundering risks than those that offer purely personal accounts, though money laundering remains a general risk for all members.

- One FFE member cited an instance in which a Belarussian individual with a Spanish address began receiving monthly high value USD payments from accounts in Cyprus. Transaction monitoring helped to detect these anomalies. Source of wealth checks the fintech conducted showed links with Thai and Russian companies involved in airline ticket arbitrage.

Case Study – Smurfing

One FFE member identified a network of smurfers. The customers met the target demographic of the product, so were not highlighted at onboarding. The customers were mostly in the company's target age range and lived in North and East London. It was through monitoring transactions and analysis of their distinct payment references that they were identified as part of a linked network. They were debit card-loading an initial small amount (£10-20), followed by multiple payments totaling £250, many from stolen cards. The funds from multiple customers were sent to one centralised customer, who then sent the money out of the network.



- PEPs: Some FFE members indicate that their customers include PEPs, even if in relatively small numbers. This requires heightened levels of due diligence and monitoring to mitigate the risk that a company could handle the proceeds of corruption.

    - Effective ID&V procedures, source of wealth checks and transaction monitoring can mitigate the risks associated with PEPs.

- Sanctioned persons: Some FFE members have encountered instances of positive matches against international sanctions lists, requiring them to deny account opening to prospective customers. Some have also detected instances of customers attempting to make payment to sanctioned persons, requiring the rejection of payments.

    - Effective screening solutions and transaction monitoring have enabled FFE members to manage these risks when encountered.

A key theme that has emerged in early FFE meetings is that criminals will target fintechs deliberately, seeking to exploit new products and services as soon as they launch. This leaves young start-up

companies particularly vulnerable to fraudsters and money launderers, who may target their immature control frameworks. Fintechs must be prepared to face these risks from the moment they go live.

Risks on the Horizon

Effective CDD can enable the identification of new risks as they emerge. As part of its ongoing work, the FFE provides a forum for fintechs to scan for potential illicit finance threats on the horizon. FFE members generally have yet to encounter the financial crime risks below on a significant scale, but are discussing methods for mitigating these threats as they emerge.

- **Terrorist financing:** Terrorists constantly evolve their methods of fundraising, and fintechs must be prepared that terrorists may target their products and services. Several recent cases have emerged of terrorists using prepaid cards and student and payday loans as sources of funding – as well as other services that fintechs provide. Terrorist organisations are also becoming rapidly more technologically adept, expanding their use of social media and other digital tools for recruitment and fundraising. Fintechs may therefore present attractive targets for terrorists. It is important as well that fintechs not limit their efforts to prevent terrorist financing to detecting jihadist activity: right-wing terrorism is on the rise and represents a threat. High-quality CDD that leverages social media data and is combined with automated transaction monitoring tools using customised rules can help to detect terrorist financing risks.

- **Tax evasion:** Smaller fintechs are unlikely to encounter attempts by customers to launder the proceeds of tax evasion in large volumes; but as they scale, fintechs could encounter attempted tax evasion using their products. This is true in particular of companies offering international payments, current accounts or services to business customers. Companies with exposure to US persons among their customer base could face consequences under the Foreign Account Tax Compliance Act (FATCA). The UK Criminal Finances Bill includes a corporate offence for companies that fail to prevent the facilitation of tax evasion. Fintechs will have to ensure they are able to deter and detect instances of tax evasion. Robust CDD and activity monitoring will be a critical component of those efforts.

- **Cybercrime:** The UK's National Crime Agency has indicated that cyber-enabled fraud has become the largest source of criminal activity in the UK. Fintechs are particularly vulnerable to these threats, as hackers look to obtain card details, target accounts to steal customer funds and compromise information contained on mobile devices. Customers' data collected during the CDD process can be jeopordised if obtained by hackers. Deterring these risks requires strong data protection practices that ensures the integrity of customers' personal information. Many FFE members, for example, use multi-factor authentication to enhance security for customers. Fintechs will also need to ensure compliance with the EU's General Data Protection Regulation, which will require that they disclose instances of compromised or lost data.

Third Party Risks: Thinking Beyond Customers

In addition to robust CDD, any risk management framework must include other components – such as thorough audit and assurance arrangements – to ensure effectiveness.

Because of their frequently small size and rapid evolution, fintechs often rely on third-party business-to-business (B2B) suppliers to provide CDD services and undertake certain functions, such as screening for PEPs and sanctions. Outsourcing of CDD processes can carry additional risks, and it is essential that fintechs conduct assurance around any third-party arrangements.

UK regulatory and industry guidance emphasises the necessity of conducting regular and thorough assurance of third party solutions and outsourced services. For example, the JMLSG advises that where they use a third-party solution, a firm "should understand its capabilities and limits, and make sure it is tailored to their business requirements, data requirements and risk profile. Firms should also monitor the effectiveness of automated systems."[3]

FFE members generally note that third party outsourcing presents an ongoing and significant challenge. Smaller firms can be heavily reliant on third party vendors for customer screening and transaction monitoring solutions; in some cases, there may be few reliable and affordable third party vendors operating in the market for certain services. Finding a suitable solution can be a matter of trial and error. Fintechs will need to establish formal assurance arrangements that enable robust testing of third party systems.

When engaging B2B service providers, fintechs should consider the following:

- ✓ Does the provider have a good reputation? What do other fintechs say about their experience with the provider?
- ✓ Does the solution have proven success?
- ✓ What is the providers methodology for the design of their systems? Is it sound?
- ✓ Does the provider regularly test their products to ensure they are regulatory compliant?
- ✓ Is the solution designed with specific local regulatory requirements in mind?
- ✓ Does the provider obtain third-party assurance testing of their products?
- ✓ Is the provider responsive to feedback?
- ✓ Will the provider work with their customers to tailor solutions?

As a starting point, answers to these questions can provide fintechs with comfort about B2B providers and their services.

In certain cases, fintechs themselves may not face direct risks of loss, theft or abuse from criminal customers; instead, third party service providers may bear the primary risks. It is nonetheless important that fintechs be aware of these situations to ensure their third-party suppliers and partners are not adversely impacted.

[3] JMLSG, Part III, Chapter IV, "Compliance with the UK financial sanctions regime."

For example, in the case study of ATM reversals discussed earlier, the fintech whose customers were engaging in ATM reversal faced no threat of monetary loss; rather, the ATM providers would bear any losses because of the fraudulent activity. It is important that fintechs be aware of these deferred risks and communicate with their third-party partners were these risks are identified to ensure the integrity of all parties.

Summary and Conclusions

Fintechs are well-positioned not only to provide a frictionless experience to consumers, but to monitor and manage customer risks in innovative ways as well.

Fintechs should aim for an approach to CDD that enables the detection and mitigation of risk without disproportionately disrupting the customer experience. Innovative approaches for conducting ID&V can help to achieve this balance.

Fintechs should also pursue an approach that enables a dynamic and holistic view of customer risk. Leveraging data from numerous sources and applying innovative analytical techniques can facilitate a dynamic approach.

Lastly, fintechs should develop CDD approaches that are sufficiently flexible that they can evolve using a risk-based approach as their customer bases and product offerings change and scale.

FFE members are demonstrating through their efforts how this balance can be achieved, and they continue to work at refining their approaches. To ensure success, it will be critical for fintechs to consider formalising governance arrangements and to develop robust assurance testing around both in-house and third party providers and services.

The FFE is committed to empowering fintechs in these efforts.