KYC Manager

Finologee & Harmoney



# DIGITALISING KYC & AML: A GUIDE FOR LUXEMBOURG-REGULATED ENTITIES

**EMBRACING DIGITAL KYC PROCESSES**
as a Luxembourg-regulated institution

**PLANNING AND OPTIMISING**
digital user journeys

**REMOTE CUSTOMER IDENTIFICATION**
for Luxembourg-regulated companies: how and why?

**EIGHT REASONS TO DIGITALISE**
KYC and AML



# TABLE OF CONTENTS


04 KYC/AML PROCESS DIGITALISATION: OPPORTUNITIES AND POINTS OF REFLECTION

05 HOW CAN KYC MANAGER HELP YOU?

08 EMBRACING DIGITAL KYC PROCESSES AS A LUXEMBOURG-REGULATED INSTITUTION

11 PLANNING AND OPTIMISING DIGITAL USER JOURNEYS

14 8 REASONS TO DIGITALISE KYC AND AML INTERACTIONS

17 HOW TO CHOOSE THE RIGHT COMMUNICATION CHANNELS TO RETRIEVE DATA FROM YOUR CLIENTS?

19 REMOTE CUSTOMER IDENTIFICATION FOR LUXEMBOURG-REGULATED COMPANIES: HOW AND WHY?

23 KYC MANAGER CASE STUDIES AND CLIENT OUTCOMES

26 OPERATIONAL EXCELLENCE: 4 REASONS WHY CUSTOMERS TRUST FINOLOGEE

28 A SELECTION OF CLIENTS

29 ABOUT FINOLOGEE

30 ABOUT KYC MANAGER: A JOINT-VENTURE BETWEEN FINOLOGEE SA AND HARMONEY N.V.



# KYC/AML PROCESS DIGITALISATION: OPPORTUNITIES AND POINTS OF REFLECTION

As the AML/CFT regulatory landscape continues to change and increases the KYC-related operational burden, for many of Luxembourg's regulated businesses, **dematerialising KYC processes is looking increasingly attractive.**

While many of Luxembourg's regulated entities are interested in digitalising their processes, companies are looking to analyse and understand the scope of work and possibilities that surround dematerialising KYC or onboarding processes in more detail.

We hope this guide will provide you with more context, and that it will help you further understand where there are **opportunities and points of reflection** when considering a digital onboarding or KYC lifecycle management solution.

# HOW CAN KYC MANAGER HELP YOU?

KYC Manager is a ready-to-use digital customer onboarding and KYC file lifecycle management platform, tailored for Luxembourg-regulated financial institutions. It helps **Luxembourg-regulated insurers, fund managers, banks and other professionals to digitise and streamline their KYC processes**, from client onboarding to KYC file update campaigns and client KYC lifecycle management, in full compliance with Luxembourg's financial industry regulations.

KYC Manager helps Luxembourg's financial institutions to optimise the management of their KYC and AML-related processes, files and data sets. Using KYC Manager, **financial institutions can connect their end-customers, front-officers and compliance department teams on the same platform**. The interface is both customer and employee-centric and covers all parts of the customer KYC lifecycle.

KYC Manager is built and operated by Finologee and its partner Harmoney. Thanks to Finologee's expertise in building and running business-critical and regulated infrastructures that are live since 2006, the Software-as-a-Service (SaaS) framework that KYC Manager is part of has been designed to meet outsourcing requirements that apply to the Luxembourg financial industry. KYC Manager is hosted in Luxembourg in EBRC's Tier IV data centres.

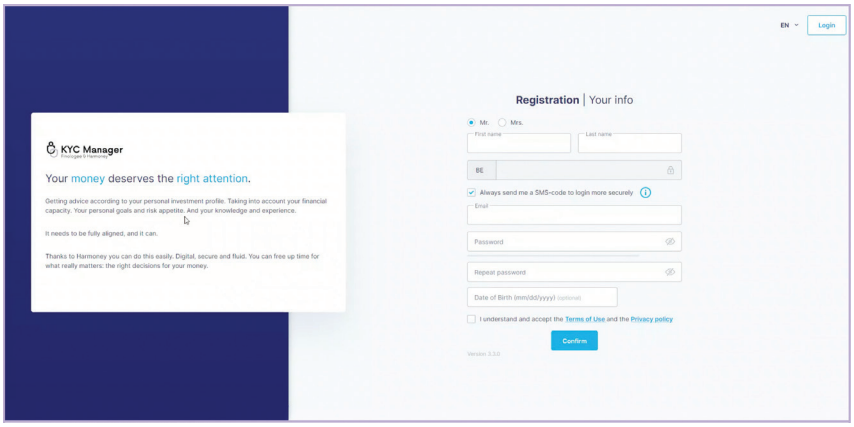
## HOW CAN KYC MANAGER HELP YOU AS A REGULATED ENTITY OPERATING UNDER LUXEMBOURG REGULATIONS?

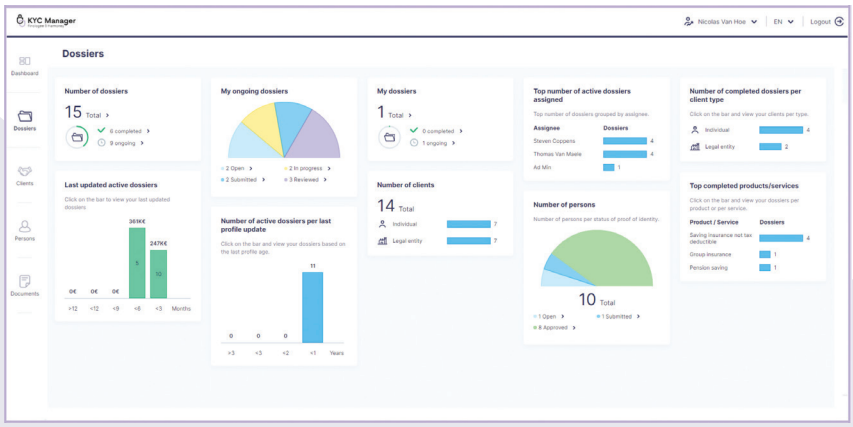
We help insurers, fund managers, banks and other professionals with a variety of aspects of their customer KYC lifecycle management. **KYC Manager can be white-labelled to offer a branded solution** that is completely integrated into your firm's individual customer experience. We can tailor KYC Manager to your needs to build a comprehensive KYC solution that meets your organisation's specific requirements.

### CLIENT KYC FILE UPDATES

KYC Manager **makes the end-client KYC review and update process swift and cost-efficient**. Using KYC Manager, financial institutions benefit from more complete and higher-quality KYC files than with traditional KYC data collection processes. Because KYC Manager makes it easier and faster for customers to provide their KYC data, keeping up to date with evolving regulatory requirements and dealing with regular KYC file updates also becomes much more straightforward.

The platform **can be extensively customised to meet regulated firms' specific KYC update needs**. Financial institutions can build personalised workflows and specify which data and documents need to be collected. **End-clients are contacted directly through the platform**, which sends an automated email message, SMS text or paper letter inviting end-users to upload KYC documentation and data, kick-starting the KYC file update process. The platform is intuitive for customers to use. **KYC updates can take as little as a few minutes**, with data being made immediately available to compliance and back-office teams.



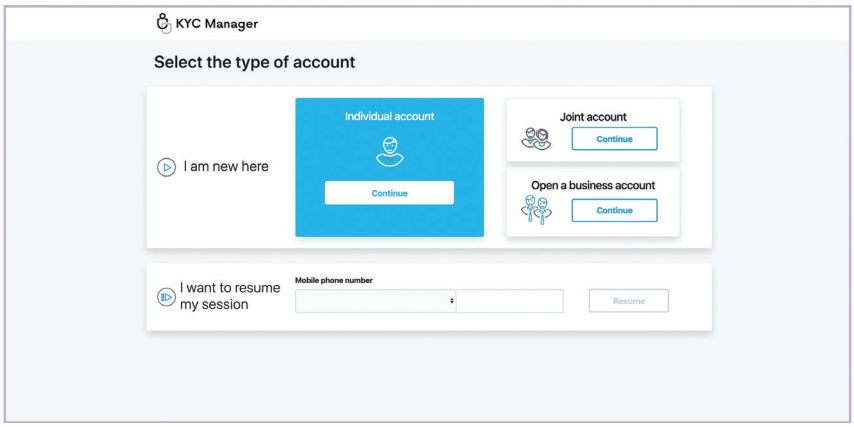




## KYC LIFECYCLE ANALYSIS

The platform provides **lifetime views of each client and allows users to carry out easy data reviews**, as well as ongoing due diligence and periodic KYC reviews. Finologee's analysis tool allows institutions to review groups of clients (through filters) or to view clients at an individual level. Risk is reduced and **staying on top of KYC at any point in a client's lifecycle becomes easier, faster and more streamlined** for both the institution and its clients.

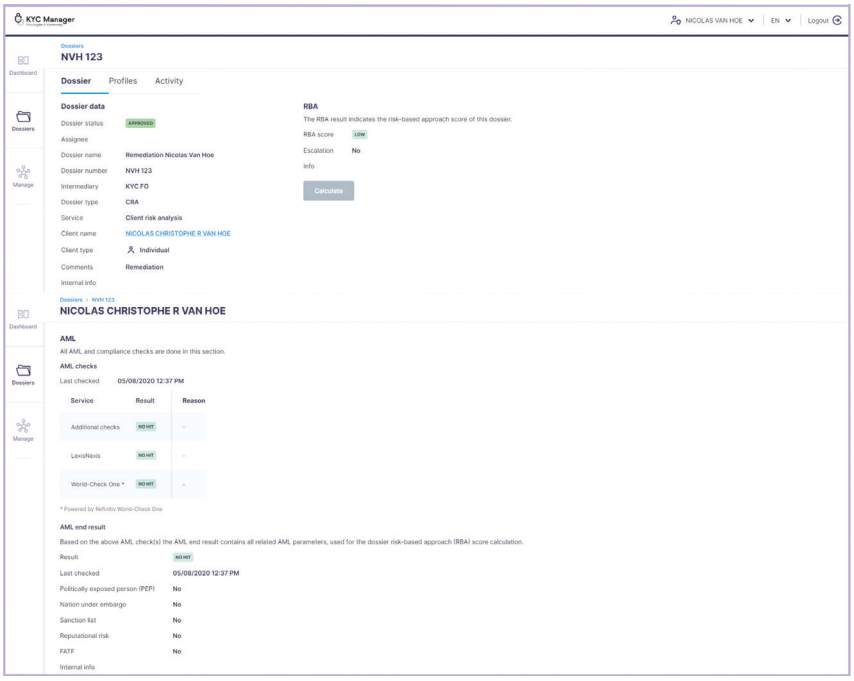
## DIGITAL ACCOUNT OPENING

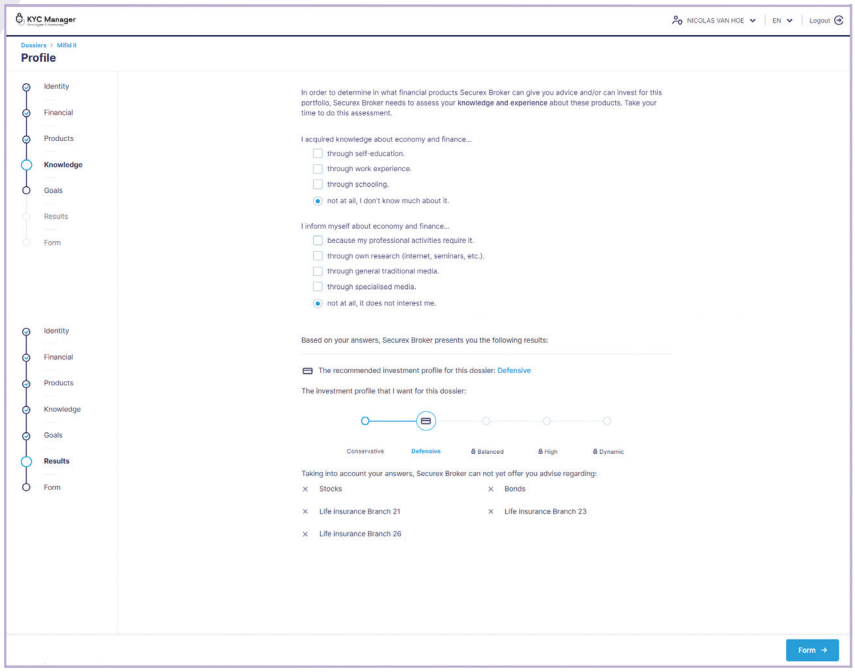
Digital onboarding of both natural and legal persons with intuitive and frictionless data and document collection becomes a straightforward process. **Front and back-office teams can handle any necessary verification and approval processes quickly and efficiently** through the platform. Because documents and data are sent digitally, **customer onboarding is simple and efficient**. Customers benefit from a fast, modern and streamlined onboarding process Financial institutions **enjoy improved conversion rates, reduced onboarding time, real-time access to data and easier risk analysis**.



## PEP/SANCTION LIST CAMPAIGN

Financial industry professionals can **easily submit a list of customer files/ records to run against one or more blacklists/sanction lists**. KYC record checks can be automated to check records against blacklist/sanction lists on a recurring basis or can be triggered manually. The platform offers complete flexibility to choose which lists KYC records are checked against. Enhanced features allow our clients to filter, export hit/no hit lists, display hit data, eliminate false positives and **export data easily for reporting purposes**.




## MIFID/IDD RENEWAL CAMPAIGN

Through KYC Manager, financial institutions can request that **end-users fill in a questionnaire to automatically define their MiFID II/IDD investor's profile**. Firms can run campaigns on selected/filtered users to update their investor profile through a branded interface, providing a trust-inspiring and modern customer experience. Notification of selected end-users through email, SMS text messages or paper letters becomes **a straightforward process, asking them to connect to the platform and update their profile when required**. Compliance and back-office teams can check details and validate end-user profiles within the system and easily export data/files as required for reporting and internal use.

**EMPOWERING FINANCIAL INSTITUTIONS.**
**SCAN FOR OUR EXPLAINER VIDEO.**



# EMBRACING DIGITAL KYC PROCESSES AS A LUXEMBOURG-REGULATED INSTITUTION

Established financial institutions are **increasingly in competition with young challenger firms**. New players are marketing themselves as savvy, digitally focussed firms offering a customer-centric approach and enhanced user experience.

There are also threats from other - once unlikely - places. Big tech companies such as Google, Apple, Facebook, and Amazon, with their databases of hundreds of millions of users, are looking to flex their muscles

and it is no secret that **many of them see significant opportunity in financial services markets**. These players are already making inroads into areas such as payment services, with some of them holding e-money institution licenses from the Luxembourg Ministry of Finance.

In the past, compliance issues have been a significant barrier to entry for financial technology providers large and small, but today their technical capabilities have largely overcome this hurdle, allowing their enhanced user experience to develop as a competitive advantage.

## DRAWING ON APIS

Challenger firms are not 'better suited' to the future than incumbent companies. Evolving and seeking out new tools will be critical to the success of established firms, but **just as new fintech firms have harnessed digitalisation, so too can established firms**.

Using application programming interfaces ("APIs"), traditional players in the financial services space can outsource processes that once required costly and not always efficient direct human involvement, for example.

How does this work? APIs act like communication channels between a company's system and a specialist provider's software solution, interlinking the two and enabling them to interact with each other. This allows for a **seamless integration of selected solutions within pre-existing processes**.

In their early days, challenger firms outsourced customer identification procedures and KYC remediation to external parties. Although leading players might now have an internal KYC system, **outsourcing remains a straightforward and default strategy for non-digital specialists**. Thanks to the industry's embrace of APIs, **institutions are able to draw on a vast number of modules, services and programs, whilst retaining control and flexibility**.

One example relates to KYC due diligence checks: through API integration, providers are already enabling Luxembourg's regulated institutions to retrieve and authenticate customers' digital signatures and ID documents efficiently and cost-effectively.

As digital transformation advances, it is likely that these tools will only be the beginning: regulated entities will eventually be able to change their operating models and fundamentally rethink the services they provide.





# PLANNING AND OPTIMISING DIGITAL USER JOURNEYS

Shifting away from traditional 'manual' processes to digitalisation is a significant change for your business. While it is an interesting proposition for many brands, where do you start when it comes to thinking about what your potential user journey will look like? Here, we cover some of the high-level aspects for you to consider that will help you map your user journey:

## MAKE SURE YOU HAVE A CASE FOR DIGITALISATION

Digitalisation offers tangible benefits for many regulated firms, but it can be time-consuming to set up, so **you must make sure it is the right option for you**.

It can make sense to review your business lines, focus and activities to see what would work best: there is no one-size-fits-all solution. You could digitalise certain processes, opt for digital onboarding only, or perhaps decide to digitalise (for instance) KYC or AML client file updates only. **The right service provider will be able to cater to your needs with a modular solution that you can tailor to your requirements**, so identify what it is that works for your business and context, before going forward.

While digitalisation is the right fit for many regulated firms, it is perfectly possible that keeping your current processes is the best and most logical solution for you and your clients. In this case, our advice typically is to stay with what is working - digitalisation for digitalisation's sake does not help in most cases.

## THINK IN DEPTH ABOUT WHAT YOUR CLIENTS NEED

**Ensuring your clients will be happy with digitalised onboarding, AML/KYC file updates and other relevant processes is critical for success**. What your clients expect from a digital solution should also be considered - ideally by getting client feedback and insights into what they would like to see from your business. Client expectations are likely to vary extensively, and it is important that you consider what will make most sense to your business, rather than trying to apply a more blanket approach.

For example, for some firms, the need for human interaction is typically low, so digitised KYC and onboarding processes are easier to introduce and are widely appreciated. For other institutions, digitised KYC may be less appropriate if your clients want a more hands-on and personal experience (which may often be the case, for instance, with high-net worth clientele). It could, however, have a role to play for certain types of processes, such as retrieving a digital copy of an ID document, or a routine file update.

## CONSIDER INTERNAL STAKEHOLDERS

While customer experience will need to be at the forefront of your planning, internal stakeholders also need to be involved. **Identify and liaise with any parties to cover the viability of the project, their needs and what constitutes a successful outcome for all**.

### REVIEW HOW OTHER COMPANIES SET UP THEIR DIGITAL JOURNEYS

In the first instance, simply following and analysing what your competitors and other service providers are doing in terms of digital KYC, AML and onboarding can get you off to a good start. **There will be plenty of publicly available information that you can analyse and consider when thinking about what would work - or what will not work - for your own customer journey**. Reviewing the competition will also help you shed light on the parts of the user journey you could refine or do differently, potentially giving you a competitive advantage.

The user journey should focus on the needs and expectations of your clients and what they want to see from you - every organisation is likely to have different requirements and what is applicable for a retail bank may not always be appropriate for a private bank, for example.

### NEXT STEPS: GETTING MORE SPECIFIC

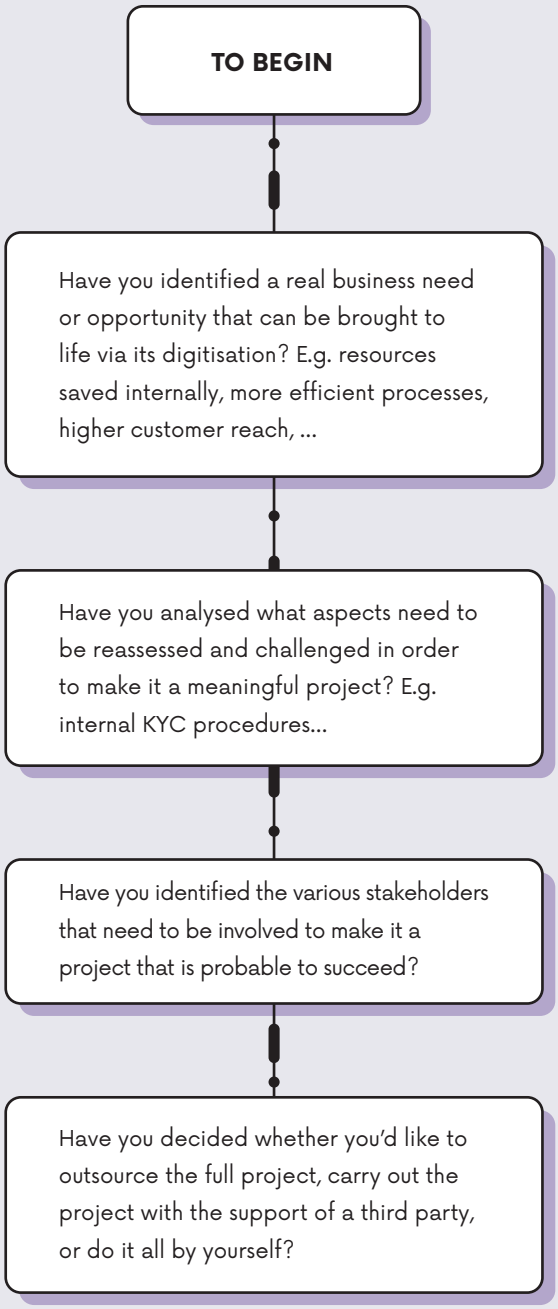
Once you have a grasp of what your clients and internal stakeholders need and what the competition is doing, you can then look more in detail at what you will need from a digitalised process. Here are some examples of questions you can ask to narrow more effectively what your user experience will look like:

- Will you pre-identify and pre-authenticate users?
- Will you use technical risk assessments of user behaviour, or not?
- Which data and information will you need to collect and analyse?
- Will you use identification methods and if so, which ones?
- What kinds of user consent will be necessary?
- How will you automate sanction lists checks?

By then, you should have a fuller idea of what capabilities you will need. You can next create a high-level map of what the user journey will look like. At this point, you will also have a clear understanding of whether it will make sense for you to build a digital platform in-house, or if you will outsource to a technical service provider.

## THE CHECKLIST

Here is a checklist to help you kickstart the process of digitising your KYC processes, such as customer onboarding or remediation:



## YOU MIGHT FIND YOURSELF IN ONE OF THESE 3 SITUATIONS

### Work with an external technical provider

- Have you identified providers that master all 3 essential areas, i.e. compliance, technical capabilities, and user experience?
- Have you compared various solutions and clarified all practical aspects when implementing digital KYC solutions with an external provider?
- Have you identified regulated providers to make sure you are compliant with the regulations that apply to you? (CSSF outsourcing circulars & EBA Guidelines on outsourcing)
- Do you want to rely on an external hosted platform or do you prefer to go for a system with components set up on premise (software solution)?

#### External provider

- Have you decided whether you want to use only APIs or do you want the provider to build your full-fledged system?
- Have you made sure the external provider has completed its due diligence with 3rd party products it is offering?

#### On premise deployment

Is there any solution that meets your requirements (build or buy)?

**If no, you need to build it**

#### If yes

Is this solution future proof, extensible and does the required (additional) effort to deploy it on premise make sense in your context?

### Do it yourself with the support of an external advisor (e.g. consultancy or law firm)

- Have you defined the scope of the mission you need an external provider's support on?
- Have you identified providers that have the necessary experience and access to resources matching your specific needs?

### Do everything by yourself

Have you defined the scope of the project and feel confident about being able to complete it by yourself?

### For both of these situations, ask yourself the following questions

- Do you have the necessary resources confirmed by top-level management to complete the project in a timely manner and high quality?
- Have you made an extensive analysis on what API providers to choose to digitise your processes (e.g. Ariadnext, IDnow, Onfido, LuxTrust, Docusign, ...)
- Are you entitled to and did you carry out a due diligence process to select those providers? CSSF Circulars, etc.
- Do you have the necessary in-house technical resources to test and integrate all chosen providers?
- Do you have the necessary user experience experts in-house to successfully keep users (prospects & clients) and their needs at the center of your digitisation project?



## BUILD CUSTOMISED KYC JOURNEYS THROUGH KYC MANAGER

Thanks to KYC Manager's modular design, **our clients can cherry-pick the components and modules they need in areas such as customer identification, sanction list screening or electronic signature**. The platform enables financial institutions to create hyper-personalised, end-to-end client and employee experiences.

Based on the needs of the financial institution, we can implement these ready-to-use components into the KYC Manager platform. By doing so, financial institutions design tailored, frictionless, and efficient digital KYC user journeys adapted to their specific KYC needs.

The KYC Manager platform helps financial institutions offer smooth and digital KYC processes such as: customer onboarding, KYC remediation campaigns, periodic KYC review, blacklist/sanction list checks, adverse media and business register/database checks and many others.

# 8 REASONS TO DIGITALISE KYC AND AML INTERACTIONS

There are quite a few reasons why digitalising KYC and AML interactions can be beneficial for your business. Here is a selection of them:

### 01
### BENEFIT FROM ENHANCED SECURITY

**Digitalised processes can strengthen your security**. Automated document verification processes can be more thorough than manual checks. Any anomalies, poor quality data and discrepancies are either flagged or not allowed into the system (in the case of a poor-quality document, for example).

As well as meeting regulatory requirements, **digital AML and KYC processes can be tailored to meet your internal risk matrix** so that you can create your own workflows, based around the risk level of the client, how you would like them to navigate through the process and the documentation that is required.

### 02
### IMPROVED DATA

With regulations continually changing, it is likely that you will need to carry out KYC and AML checks more and more often and more thoroughly in the future. At the same time, document quality is a concern: you want accurate data and records for your files and regulators are also demanding exceptionally good quality documents to limit risk.

Despite the need for better quality documents, using traditional KYC and AML collection methods, clients often inadvertently send poor quality documents. Poor copies, blurred imagery and unclear data that can trigger lengthy manual processes to seek out better quality documents. The collection process then needs to be started again, risking delays and unhappy clients who do not always

understand why they are being asked to send the same information a second time. **Digitalised KYC and AML processes can increase quality because software automatically analyses and checks incoming data submitted by your clients for clarity and quality. Documents that are not appropriate quality for your needs are rejected before they can make it into your systems**. Clients can only upload clear documents, and it is easy and quick for them to do so.

## 03
### REDUCED HUMAN ERROR

Manual-heavy processes can leave room for clerical errors, especially when your teams are uploading client KYC data by hand into systems, as is often the case in traditional AML and KYC onboarding and update processes.

Machines can do more than simply reducing administrative errors and transferring data correctly into your systems. **Identification processes are highly sophisticated and spot discrepancies that may not be noticeable to the human eye**. Image analysis software that compares a person's ID document with a photo or video and related sophisticated algorithms can be more efficient in spotting potential inconsistencies, for example.

## 04
### DIGITAL EVIDENCE

Because of their very nature, KYC and AML systems also give you more digital evidence. **Using electronic data trails and logs, it is easier to prove that you have appropriately executed due diligence and client file update campaigns**, especially if you use timestamping and electronic signatures.

You are legally required to store documents as evidence that you have carried out due diligence, and these are easy to classify and keep in dematerialised form.

## 05
### SIMPLIFIED REPORTING

Understanding the overall status of your client files, which documents need to be updated and files that may need to be verified more regularly can be challenging if you are dealing with paper files and non-automated reporting. **When your records and customer due diligence is digitalised, data is easy to compile and regroup into different reports - everything can be viewed and exported at the click of a button**. Files which need to be updated, campaign dashboards and the status of all or some of your data is at your fingertips with simplified search and reporting functionality. Searching for certain types of files, based on your needs, is also easy thanks to filtering options.

## 06
### REDEFINE CUSTOMER EXPERIENCE

Fully remote relationships may not be suitable for every business; if you are a private bank, for example, your clients may appreciate a hands-on and personalised interaction with you. On the other hand, retail banks may find that customers want fast and efficient onboarding and KYC/AML update processes that take a minimum of time to complete.

There are ways to cater to both scenarios. For firms, whose clients want a more hands-on experience, initial client onboarding can take place at an in-person meeting. Additional digital identification checks can be carried out remotely as a second step. KYC and AML updates can then either be digital, in-person or an appropriate combination of both. For regulated firms where fully remote client identification and KYC file updates are the best options, all processes can be digitalised, redefining the customer experience and interactions.

## 07
### SIMPLIFICATION OF LIFECYCLE IDENTITY MANAGEMENT AND REMEDIATION CAMPAIGNS

Digital identification tools can make it easier to manage, review and carry out KYC and AML campaigns. **A digital platform such as KYC Manager will allow you to send remote requests on an ad hoc or regular basis to specific customers and clients**. These can either be to comply with periodic review obligations or to carry out targeted digital AML and KYC updates of customer files.

## 08

## A SINGLE PLATFORM FOR YOUR CLIENTS, COMPLIANCE, AND YOUR FRONT AND BACK OFFICE

Onboarding clients and collecting KYC and AML often involves multiple parties in-house. While your compliance teams are ultimately responsible for ensuring you are operating in line with regulations, using traditional onboarding and document collection methods, they typically do not liaise with clients directly. Instead, they rely on front office teams who collect necessary documentation, completing client AML and KYC files.

For their part, client-facing teams are doing their best to compile the right KYC and client information, but they are hampered by client delays, reception of documents of varying degrees of quality and documentation being sent in multiple different formats (in-person, via email, post, etc.) and then manual update processes. The result is that while KYC and AML client file updates are being carried out, your business has little oversight of the completeness and progress of campaigns.

Digitalising client onboarding and KYC and AML updates streamlines the process for all parties. **Compliance retains control of the campaigns and they can set up new campaigns as regularly as they need**. They can send reminders and follow-ups as regularly as needed. **Front office teams have access to the same system and viewing rights of relevant client files, allowing them to see if clients have updated documents** and giving them the ability to remind clients if they have not when they are interacting with them as part of their usual activities. Relevant back-office teams also have access to the system as required.



# HOW TO
# CHOOSE THE RIGHT COMMUNICATION CHANNELS TO RETRIEVE DATA FROM YOUR CLIENTS?

Digital account opening and KYC/AML client file updates have traditionally been carried out in a variety of ways. In the past, in-person meetings at branches or the client's home, postal delivery and email are all commonly used to collect documents. 'Wet ink' signatures were often a necessity, and this meant that physical documents were aplenty, along with the paper trail that came with them: physical receipt, filing, manually updating your systems and so on.

**Today, digital onboarding and client file updates can be triggered through email messages, SMS texts or even through paper letters leading to an online form, requiring nearly no in-person interaction**.

While we often hear of the pros of digitalisation, are there any negatives to consider? Are there also ways to combine different channels to improve conversion rates or tailor interactions to your business and clients? Here are our insights:



## PAPER MAIL

Collecting documents (signatures, ID, account opening forms etc.) has been the norm for many years. Sending documents through the mail can take considerable time to receive responses and they typically require a lot of manual data input.

Practically, most of your customers are likely to prefer different methods to sending and receiving account opening or KYC/AML update documents by post.

That said, it should be noted that sending documents in the post remains important for older client age groups who might not be as comfortable with or trusting of technology as younger generations. Anyone without a smartphone or email also tends to prefer interactions by post – or alternatively, in person – and it is highly likely that you will need to retain some capability to collect documents and signatures by post and input them into your systems.

Official mail from your institution is highly likely to be opened and read attentively by your clients, however. **Many financial institutions choose to send initial login KYC and AML remediation platform details to existing customers by mail because of the extremely high conversion rate and attention paid to relevant postal mail**. Official mail is an inherently secure channel, making it ideal for sending access details and instructions for new digitalised processes.



## COLLECTING DOCUMENTS FACE-TO-FACE

Some sweeping statements would suggest that all clients are open to digitalisation and that collecting documents manually is a thing of the past. However, for many customers, a face-to-face and highly personalised interaction is actually preferred in quite a few contexts. High-net worth clients onboarding at a private bank or subscribing a life-insurance policy could fall into this category, for example.

That said, the client of a large retail bank, for example, where a less personalised approach is more

the norm may be likely to find manual document collection cumbersome to the degree that it can impact conversion rates. Electronic signatures, digital onboarding and digital updates of KYC and AML files can be an ideal alternative.



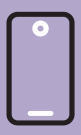
## EMAIL

Email has facilitated client interactions to some degree, allowing clients to send copies of their ID to regulated institutions quickly and easily in some scenarios, for example.

While your customers are likely to enjoy an ability to send documents digitally, email isn't necessarily an all-encompassing option in some scenarios. For instance, providing original paper documents is often still required even if copies have been sent by email. And even if electronic copies are appropriate for the matter in question, email typically is a non-encrypted and non-authenticated channel, and most of the time, it still requires manual work to upload documents and input data manually to your systems. The quality of documents provided can also be an issue as no validation is carried out before submitting.

**Where email really comes into its own is in client communication and providing a gateway to your digital onboarding and KYC/AML update platforms.** It is also a highly effective way of communicating with clients, for example notifying them of a KYC or AML client file update campaign that they need to respond to. KYC platforms often allow you to create campaigns and send notifications to clients (either all clients or just a selected group, based on your requirements) at the touch of a button. You will be able to track actions clients have taken, and provide evidence that you have launched a campaign with a digital record of the steps you have taken to contact clients. The same tracking using paper letters, for example is only possible with rather costly registered mail.

Email is one of the most commonly used channels of communication with clients to trigger KYC client file updates.



## SMS

SMS text messages can be a very efficient channel for client file update campaigns and for security. While it is a relatively new channel for client communication, **text messages have increasingly come onto the scene as a result of one-time passwords (OTP). SMS can also be used to notify clients that a client file update has been launched.** The downside of this channel can be its perceived casualness: as text messages are typically limited to 160 characters and are commonly used for quick and straightforward communications, financial industry professionals sometimes refrain from using them when a higher level of formality is required. Even though SMS texts are also unencrypted, they provide a higher level of security compared to email messages as entry points and number allocation is managed by mobile operators.



## COMBINING DIFFERENT CHANNELS

While each channel has pros and cons, it is important to note that **you do not have to pick a single or specific channel for all contexts and purposes.** Likewise, KYC Manager allows you to switch between channels depending on your campaign and available contact information: one remediation campaign might be better suited to email and another to SMS and **you will have the flexibility to choose between each channel as required.** Client preferences and context are other factors that may determine the use of a particular channel. Also, changing channels can come in handy when escalating client notification, to increase efficiency and conversion rates.

A mix of digitalisation and non-digitalised approaches can also work well. We have seen financial institutions use paper letters to launch KYC updates with great success, for example: clients were informed of the KYC file update campaign via paper mail and received their credentials to access the KYC Manager platform in a letter. Combining two channels can also work; you could opt to send an initial email launching a client file update campaign, followed by SMS communications as reminders, for instance.

# REMOTE CUSTOMER IDENTIFICATION FOR LUXEMBOURG-REGULATED COMPANIES: HOW AND WHY?

The AML/CFT regulatory framework applicable to the EU and Luxembourg's finance, banking and insurance sectors has evolved rapidly over the past few years. Also, as remote working and fewer face-to-face interactions have quickly become the norm since early 2020, companies have moved to facilitate remote interactions with clients. Internal processes have also been adapted to balance remote workforces and sometimes a complete absence of client visits.

This context prompted the CSSF, in April 2020, to call upon regulated entities to "...use financial technology (Fintech) to manage some of the CDD (Customer Due Diligence) issues presented by COVID-19..." (CSSF Circular 20/740).

Independently, new AML regulations were also introduced during the summer of the same year (CSSF Regulation No 20-05 and CAA Regulation 20/03). **While this new legislation created new obligations for the Luxembourg financial industry, it also presented new possibilities, notably relating to remote customer onboarding**.

## HOW HAVE REGULATORY CHANGES MADE REMOTE CLIENT IDENTIFICATION EASIER?

Client identification is usually the first stage of customer onboarding. Regulated players in the financial industry are required to gather identification information on all their customers using at least one valid, authentic official identification document. Periodic verification, updates and remediation campaigns then follow throughout the customer's lifecycle.

The **CSSF Regulation 20-05 and CAA Regulation 20/03 now provide further flexibility for carrying out client identification remotely**, which until now, had been challenging from a regulatory perspective.

Clear guidance has notably been introduced on **permitted means of electronic identification (which can now be used without triggering an automatic presumption of higher risk)**. These are either: (i) eIDAS trust services (as detailed in Regulation (EU) No 910/2014, better known as the "eIDAS Regulation") or (ii) "Any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities."

The latter generally refers to digital processes integrating tools such as video chat, automatic ID document recognition and validation (with technologies such as MRZ scanners) and others. While the CSSF or CAA could, theoretically, 'pre-approve' some solutions, it is most likely that discussions would be needed on a case-by-case basis, due in particular to the complex nature of AML verifications and the need to tailor processes to each company's needs and requirements.

**Fully automated onboarding with no human verification is also now possible** in certain cases (i.e. for low risk profile prospects) and under certain conditions (i.e. sufficient efficiency and reliability, regular review of robustness, alignment with internal AML policies, etc). CSSF Regulation 20-05 details that such automated processes should comply with further guidance issued by regulatory authorities, whereas CAA Regulation 20-03 expressly requires CAA approval. Conditions therefore remain strict.

## WHAT CRITERIA SHOULD YOU CONSIDER WHEN SELECTING OR BUILDING DIGITAL IDENTIFICATION PROCESSES FROM A COMPLIANCE PERSPECTIVE?

The regulator's stamp of approval aside, you should make their own independent assessment as to the adequacy of a potential digital identification solution. You will need to explore all criteria extensively, but here are some of the questions and considerations you should think about:

### SECURITY

How secure is the system? How are communications encrypted? What other technical measures have been taken to mitigate risk of unauthorised access or reduce the risk of fraud? Are sufficient technical controls carried out? If you are relying on an electronic identification scheme (eID), eIDAS provides three assurance levels (low, substantial, and high) which give an indication on the level of reliability/security.

### ROBUSTNESS, EFFECTIVENESS AND RELIABILITY

These are criteria specified by the CSSF in respect of automated onboarding requirements; they should generally apply to all remote identification processes.

### CLARITY OF INSTRUCTIONS PROVIDED TO CUSTOMERS

This should also take into consideration any **required consents**.

### INTERNAL PROCESS

How will you ensure your internal procedures support the use of outsourced processes? What might need to change internally to meet new requirements?

### DUE DILIGENCE

Performing appropriate due diligence on external providers you plan to use is a must. You should also consider how you will perform due diligence on the whole outsourcing chain (in line with general outsourcing regulatory requirements).

### SECURE AUTHENTICATION MECHANISMS

Use of secure authentication mechanisms in support of the process and for lifecycle identity management, e.g. two-factor authentication (which can include, for example, SMS one time passwords (OTP) and/or biometric authentication means).

## OUTSOURCING TO IMPLEMENT REMOTE IDENTIFICATION: REGULATORY CONSIDERATIONS

When implementing electronic identification processes, it will not always make sense for you to build an in-house system. In-house platforms can be costly and not all businesses have the capability or resources to build one from scratch. **Turning to a third-party provider whose core business is designing secure technological solutions can be an ideal solution.** However, this should be done carefully. Luxembourg's regulators emphasise that as a regulated entity, you must retain ultimate responsibility and authority over your AML processes, and you will also be responsible for the ultimate control of your KYC processes.

### DECIDE WHAT KIND OF OUTSOURCING IS BEST FOR YOU

Before thinking in more detail about the 'how', the outsourcing process will start with defining what 'outsourcing' actually means for your business. For example, is it the remote identification process itself that is delegated to a third party or is it just about finding a partner to provide digital tools that will enable you to carry out the process yourself using these tools?

### FULLY OUTSOURCED AML: A THIRD PARTY CARRIES OUT CUSTOMER IDENTIFICATION

New regulations have tightened financial industry professionals' obligations when they rely on outsourced AML processes. In particular, these regulations target situations where a third party fully or partially carries out customer identification. An example is when an entity has developed electronic identification processes and offers to operate as an introducer/delegate for a regulated entity using this setup. Given there is a higher risk due to potential loss of control, applicable legal conditions are strictly set out in relevant AML regulations for such a set-up.

### PARTIALLY OUTSOURCED AML: WORKING WITH A TECHNICAL SERVICE PROVIDER

The second option is for you to restrict the role of a service provider to the technical implementation of products/services, operating under your instructions and control. Here, the sub-contractor is neither considered a third-party introducer nor a delegate, but merely a technical service provider. This type of 'softer' KYC outsourcing is subject to general outsourcing regulations, such as CSSF Circulars 12/552 and 17/654 (as amended) and the EBA Guidelines on Outsourcing Arrangements for the financial industry, or Solvency II requirements and EIOPA Guidelines on Outsourcing to Cloud Service Providers for the insurance industry.

## WHEN SHOULD YOU THINK ABOUT COUPLING REMOTE IDENTIFICATION WITH A FULL KYC MANAGEMENT PLATFORM?

Of course, remote client identification is only one piece of the puzzle, and you may also be looking to streamline your customer experience and back-office and compliance team's digital capabilities more broadly. A full KYC management platform can facilitate customer lifecycle management from a KYC/AML perspective.



Updating documents for existing clients, running checks against PEP and sanction lists, fuller data reviews, on and off-boarding can be simpler with a full KYC Manager platform. Such platforms can cater for easy interactions between customers, back-office and compliance staff and can simplify the creation and management of customer profiles.

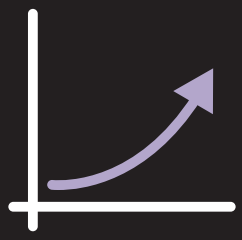
### WHAT CAN BE INTEGRATED INTO A FULL KYC PLATFORM?

- Customer risk classification
- Request additional documents, information and data required from customers based on their risk profile
- Automate reminders when client data verification needs to be carried out
- Change and manage how often checks are carried out based on the client's risk profile
- Interfacing with public registers and data providers to verify obtained data against publicly available information (e.g. blacklists/sanction lists...);
- Additional modules tailored to your needs per your own customer onboarding and lifecycle management process

# KYC MANAGER:

## CASE STUDIES AND CLIENT OUTCOMES

**FINOLOGEE AND ITS PARTNER HARMONEY HAVE HELPED REGULATED ENTITIES TO:**



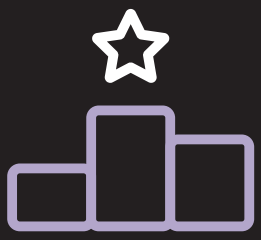
CARRY OUT A LARGE SCALE DIGITAL KYC CLIENT FILE UPDATE CAMPAIGN WITH A >50% CONVERSION RATE AFTER 2 ½ MONTHS



REDUCE THE KYC DATA VALIDATION AND SUBMISSION PROCESS BY END-CLIENTS TO LESS THAN 10 MINUTES



PROVIDE A 100% DIGITAL ACCOUNT OPENING PROCESS WITH NO PAPER/PRINTING REQUIREMENTS



DOUBLE CONVERSION RATES COMPARED TO TRADITIONAL KYC REMEDIATION PROCESSES WHILE SUBSTANTIALLY LOWERING HUMAN EFFORT AND WORKLOAD




AG2R LA MONDIALE
La Mondiale Europartner

# SUCCESS STORY – LA MONDIALE EUROPARTNER

Leading Luxembourg life insurer, LA MONDIALE EUROPARTNER (LMEP) has been using KYC Manager to run a client KYC file update campaign, reaching **50% completion in just ten weeks for the client base in scope**. Using the platform, **LMEP has reduced the KYC submission and validation process to less than 10 minutes**.

With Luxembourg's insurance firms increasingly under pressure to adhere to more stringent and regularly revised regulations, updating client KYC files more regularly was becoming a necessity for LMEP.

LMEP looked to KYC Manager for a digital client file update solution that was future-proof and customer-centric. They also wanted to improve response rates, reduce partial and incomplete data, poor quality documents and use less manpower to process paper forms.

Using KYC Manager, LMEP has been able to shape a flexible and fully customised customer KYC file update campaign. It has moved to a **digital, paperless process that optimises the management of KYC files and substantially improves the quality of client data**.

LMEP relied on KYC Manager to establish a standardised workflow that benefits the company's brokers and distributors, its compliance department and of course its customers. Each client has access to a dedicated digital profile to easily update or confirm its personal information, while the LMEP compliance team **can live-track the campaign through its KYC Manager dashboard and review customer KYC files' completeness at the touch of a button in a single location**.



Bâloise Assurances

# A HARMONEY SUCCESS STORY – BALOISE BELGIUM

In Belgium, Baloise Insurance relied on our partner Harmoney and quickly **achieved a conversion rate of 80% when carrying out a digital data update campaign on more than 240'000 clients**.

Baloise originally looked for a digital client file update process when new compliance rules came into force in Belgium. Baloise specifically wanted a solution to update client files in a way that would allow the collection of high-quality KYC data as quickly as possible. In particular, the company wanted to remove the roadblocks that typically come with manual KYC data collection processes, such as time-consuming sending and processing of (paper) forms, low response rates and incomplete, partial or poor-quality data being submitted by clients.

Baloise worked with Harmoney for the client file update campaign, **using a pre-integrated solution that was ready-to-use** for the project in question. Given the time constraints placed on the client file update phase of the project, Baloise sent letters directly to 240'000 customers requesting the additional KYC data required under the new regulations and a large number of these customers chose the option to digitally submit the relevant documents through Harmoney's white-labelled platform.

**The digital solution resulted in KYC files being better structured, and Baloise saw a significant increase in the quality of the data provided**.

Baloise later decided to continue to rely on Harmoney's KYC solution to continue to manage client files and data in a centralized and shared database Baloise's brokers, compliance and operations departments and internal audit teams are all using the platform and benefit from having an efficient, fast and digital onboarding and client file management solution that serves the needs of all stakeholders and allows them to collaborate efficiently.

# OPERATIONAL EXCELLENCE
# FOUR REASONS
# TO RELY ON FINOLOGEE

Balancing innovation with operational resilience has always been a strategic focus throughout the development of Finologee. Over the past 15 years, Finologee and its sister and predecessor companies within the same group have adjusted and scaled our operations to meet the challenges of rapidly changing business conditions, while providing the operational resilience expected by financial service professionals and institutions. A comprehensive state-of-the-art stack of procedures helps us offer highly efficient levels of support and responsiveness to our customers, laying the foundations for sustainable and long-term collaborations.

Based on customer feedback, here are **four reasons why customers choose to work with us** from an 'operational excellence' perspective:

## #1 TRUST

### FINOLOGEE OPERATES UNDER A FULL 'SUPPORT PFS' LICENSE FROM THE LUXEMBOURG MINISTER OF FINANCE

The company operates under a **double 'Support PFS' licence** granted by the **Luxembourg Minister of Finance** as both 'IT systems & communication networks operator' and 'clients communication agent' (art. 29-3 and art. 29-1 of the 5 April 1993 Law on the financial sector)

**Luxembourg**-regulated financial industry professionals are thus able and **authorised to fully rely on Finologee's** products and services for handling sensitive customer data and for outsourcing their processes. Under Luxembourg law, Support PFS are subject to the same scrutiny, audit and supervision principles and reporting requirements as other regulated financial service entities.

Finologee's IT infrastructure, business continuity/disaster recovery plans (BCP/DRP), operational procedures, data protection policies and all other relevant processes and infrastructures are compliant and audited under Luxembourg financial industry laws and regulations. This control and auditing structure is based on the '**Three Lines of Defence**' – a framework widely implemented in the financial industry to facilitate an effective risk management system. Finologee therefore has its own compliance, risk management and internal audit functions (with the internal auditing outsourced to a Big Four auditor), as well as an external auditor.

## #2 RESILIENCE

### FINOLOGEE'S INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) IS ISO27001 CERTIFIED

**Finologee has been granted ISO/IEC 27001:2013 certification**, the international standard outlining best practices for information security management systems. This certification is a cornerstone of Finologee's operational excellence strategy, aimed at providing clients with an operations infrastructure and processes for their products and platforms that meet the highest international standards, and facilitating the financial industry's quest for optimisation and innovation without compromising service quality and security.

The implementation of the ISO/IEC 27001:2013 standard establishes a robust foundation for the application of the latest regulatory requirements from national and European financial industry authorities. This enables Finologee to further **enhance** its formal **risk management** methodology processes, including **complying with recent updates to national regulations** such as CSSF Circular 12/552 and CSSF Circular 17/654, and the EBA guidelines on Outsourcing and ICT risks (CSSF Circular 20/750) covering governance, risk assessment, information security, ICT operations management, business continuity plans, and assistance to payment service users, among other topics.

# #3 CUSTOMER SERVICE EXCELLENCE

## FINOLOGEE PROVIDES FIRST CLASS CUSTOMER SUPPORT SERVICES TO MEET OR EXCEED CLIENT EXPECTATIONS

**Finologee's customer support draws on 15 years of experience building and operating high performance and business-critical platforms** for a vast community of financial industry professionals and other institutions. Among these platforms are Mpulse, handling 95% of Luxembourg's SMS payments and critical notification services, and Digicash, retail banks' mobile payment app and system which is used by more than 30% of the population.

One of the important principles guiding the support service layers Finologee provides is the commitment to guarantee a level of responsiveness that accurately meets – and ideally exceeds – customers' expectations. By ensuring **fast response times** with the help of **state-of-the-art monitoring systems, dedicated teams and 24/7 availability**, when handling incidents and throughout the lifecycle of client requests, Finologee manages to achieve a high level of customer satisfaction. In this context, the company's support teams commit to exchange information on a regular basis with customers to ensure all relevant data is shared accurately and in a timely fashion.

Finologee's proactive monitoring strategy reduces the number of issues and incidents significantly, as well as averting reactive situations. Through **high levels of automation** and automated testing that **minimise downtime** spent dealing with incidents, Finologee can instead focus on assisting customers in achieving their business objectives.

# #4 ENABLEMENT

## FINOLOGEE OFFERS DIFFERENT LEVELS OF SLA'S TO MATCH THE REQUIREMENTS AND PRACTICES OF ITS CLIENTS

**Finologee offers a progressive three-tier SLA framework based on market best practices**, able to meet different customer requirements: 'Standard', 'Enterprise' and 'Premium' (with an optional 'Financial Services Compliance' pack).

While the **'Standard' SLA** already meets most customers' expectations, the more advanced **'Enterprise'** and **'Premium'** plans are chosen by customers requiring even higher guarantees and faster response and resolution times. These plans also offer priority access to support engineers and advanced levels of incident resolution and reporting-related services.

An **efficient monitoring system** is essential when aiming for true high-availability levels. Finologee relies on sophisticated monitoring systems, based on a modern technology stack, to continuously measure events and alerts that may jeopardise availability targets agreed with customers.

Finologee has also set up its own **'change request' management process** for its products and services, offering clients the ability to request changes in the form of a service request, with full lifecycle management of products and the ability to request the delivery of a new release or upgrade of products and applications. This is backed by best-practice agreements covering suitable framework and responsiveness commitments.

Finally, Finologee provides a **complete set of reporting documents**, such as service levels reporting, service availability reporting, performance reporting and compliance reporting as well as custom reports, delivered at agreed intervals.

## SOME FACTS & FIGURES

**25M**
TRANSACTIONS PER YEAR

**45**
FINANCIAL INSTITUTION CLIENTS

**2**
ISO 27001 CERTIFICATION & 'SUPPORT PFS' LICENCE

**99,96%**
AVAILABILITY OF PLATFORMS

**14**
AWARDS & PRIZES SINCE 2010

**140**
CORPORATE & SME CLIENTS

**6**
ABBL, APSI, FTL, LHOFT, ALFI, ACA AFFILIATIONS

**12%**
REVENUES GROWTH YOY ('20-'21)

**40**
TEAM MEMBERS

Scope: Global figures NGFS Partners Group, including Finologee – 2021

# A SELECTION OF CLIENTS

A selection of clients (banks, insurance companies and others) that rely on Finologee's platforms:

(Scope: all Finologee products and platforms)

# ABOUT FINOLOGEE

Finologee is a fast-growing **digital platform operator** of robust, ready-made, and compliant systems and APIs for open finance, digital onboarding, KYC lifecycle management, professional payments as well as telecom routing and micropayments.

The company was launched in 2017 to deliver compliant cutting-edge technology with a reliable user experience. Finologee already serves **more than 100 banks and institutions** and handles more than 25 million transactions, messages and end-customer interactions per year on their behalf. Finologee draws on this deep experience in building digital platforms and ecosystems from scratch. Today, our **40 staff** support KYC lifecycle management, e-signatures, account aggregation/ payment initiation, corporate payments and secure open finance APIs for clients in more than 19 countries.

Its revenue increased by **49% YoY from €8.5 million to a total of €12.7 million** (2021-2022, at group level). Finologee is a regulated company with an IT Provider and financial data communications license by the Luxembourg Minister of Finance and is also **ISO/IEC 27001** certified.

### BANK COMPLIANCE

PSD2

All-encompassing offer to comply with PSD2 and RTS on Strong Customer Authentication (SCA).

CEDRS

Hosted gateway for account & safe-deposit box holders reporting (CSSF Circular 20/747).

### KYC

KYC Manager

Ready-to-use modular digital customer onboarding and customer lifecycle management solution.

### PAYMENTS

ENPAY

SWIFT-connected business payments management on all your bank accounts with secure API & web interface.

### PLATFORMS

mpuise.

Luxembourg's national SMS routing and direct carrier billing/micropayments platform.

DIGICASH® MOBILE PAYMENTS

Provides components and operations for the Luxembourg retail banks' payment scheme.

# ABOUT

## KYC MANAGER: A JOINT-VENTURE BETWEEN FINOLOGEE SA & HARMONEY N.V.

KYC Manager is a joint venture between Finologee and Harmoney. Finologee is a Luxembourg-based Fintech company, and Harmoney is a Belgian KYC specialist.

KYC Manager is a digital onboarding and KYC file lifecycle management tool. Finologee and Harmoney created KYC Manager to empower Luxembourg's financial institutions to transform the way they manage the KYC of their clients. Using KYC Manager, financial institutions can create personalised digital user journeys covering all aspects of the KYC and AML lifecycle. Built with compliance in mind, KYC Manager's setup enables users to meet all obligations of the highly regulated financial industry.

Harmoney was established in 2018 and works with many high-profile customers in Belgium. They operate a ready-to-use and pre-integrated solution built on secure software to ease KYC file lifecycle management. Finologee locally hosts the product as a "PSF du Support" (a licence granted by the Minister of Finance).

# GET
# IN TOUCH

**KYC MANAGER CAN EMPOWER FINANCIAL INSTITUTIONS ON THEIR KYC & AML DIGITALISATION JOURNEY.**

## WWW.FINOLOGEE.COM

For more information, please contact our sales team:
**INFO@FINOLOGEE.COM | +352 27 75 08 1**

© **Finologee S.A.** | 7, rue Jean Fischbach L-3372 Leudelange Luxembourg | **RCSL** B217.853 | **EU-VAT** LU 2966 0355
**PSF de Support** licence number 06/19 | **Autorisation d'Etablissement** N°10082748 | **ISO** 27001 (IND.20.602/IS/U)

Finologee
Digital Finance