Finologee ENPAY

COMPLIANT PROFESSIONAL PAYMENTS

MULTI–BANK & ACCOUNT INITIATION, E–SIGNATURE & AUTOMATION

WHAT IS ENPAY AND HOW IT WORKS
everything you need to know

NINE REASONS WHY
you should choose a multi-bank platform

NEW FEATURES TO DISCOVER
for compliant business payments & counterparty management

RISK MANAGEMENT & COMPLIANCE
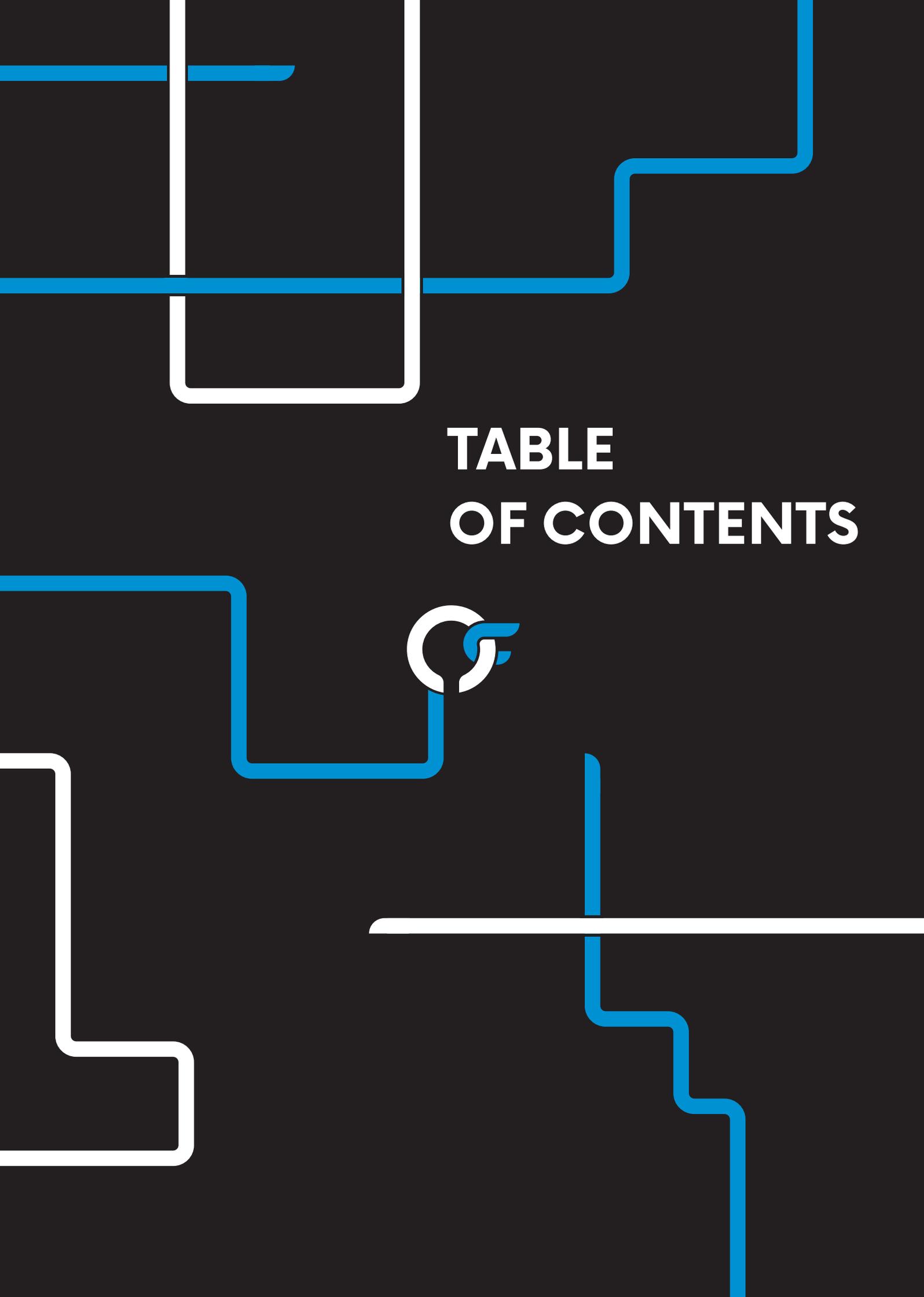discover KYC/AML screening & monitoring features

TABLE
OF CONTENTS

Table of **contents**

DISCOVER⁺
NEW ENPAY FEATURES

Vincent Arnal
CIO at LALUX

Georges Berscheid
Co-Founder & CTO at Finologee

RISK⁺
MANAGEMENT
FOCUS:

PAYMENT⁺
PROCESS
RELATED REGULATORY
CHALLENGES

READ MORE ON ENPAY.LU

| Payments	Risk Management	Reports
IN & OUT WORKFLOWS E-SIGNING	COUNTERPARTIES AML SCREENING FRAUD PREVENTION	ALL TRANSACTIONS BALANCES ASSETS

WHAT IS ENPAY
AND WHAT DOES IT DO?

FinologeeENPAY is a **professional payments** and **multi-bank account access** management **platform**. Hosted in a software-as-a-service (SaaS) setup with Luxembourg's leading data centre operator EBRC, it is designed to **enable financial industry professionals**, companies seeking flow automation as well as institutional and intermediary players to streamline and monitor their **payment initiation, validation** and **reporting workflows.**

With ENPAY, clients can efficiently access **all payment account balances, transactions** and reports from **any** of their existing **bank accounts in one place**. Thanks to its **direct connection** to the **SWIFT** financial messaging network and direct connections with selected banks, the platform allows for virtually **unlimited bank reach** around the world.

Flexible **access rights** and roles, complex **workflow** management capacity, a secure **multi-factor authentication** system and compliant **audit/reporting** capabilities provide a comprehensive gateway for financial industry and institutional players, encompassing **all core banking payment functions** via a **single secure web interface or API.**

Additionally, **Finologee's Peppol Access Point** can be used for **exchanging invoices and documents with public authorities and institutions**, as well as for **business-to-business and business-to-consumer workflows.** The aim is to enable companies to use the Peppol network to transmit messages such as invoices and orders more efficiently and securely.
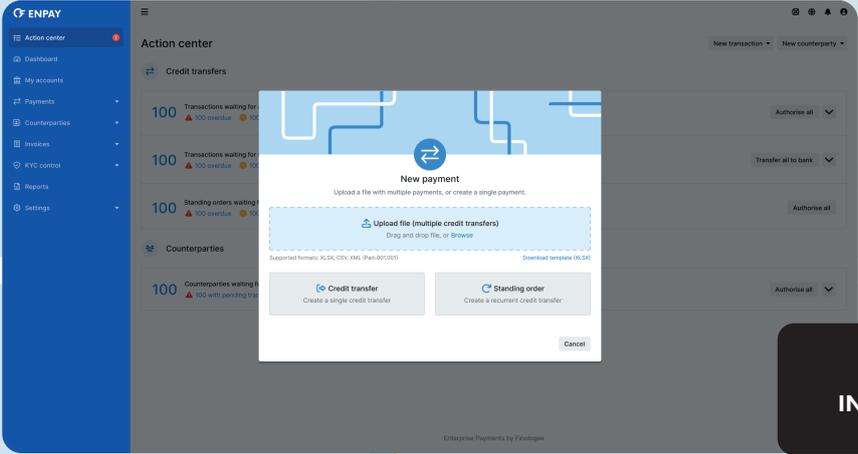
01.
INITIATE A PAYMENT
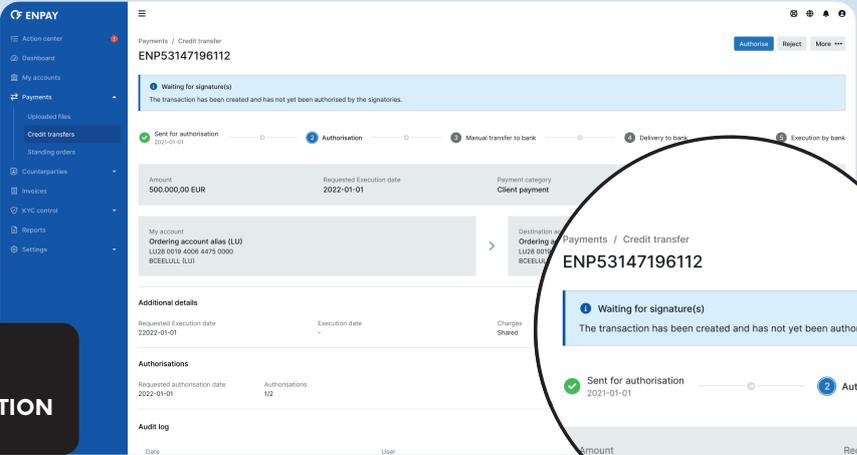
02.
AUTHORISE TRANSACTION
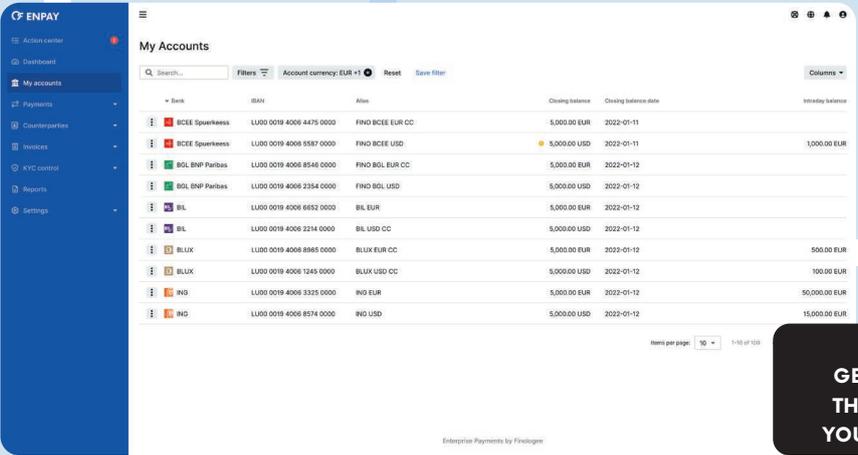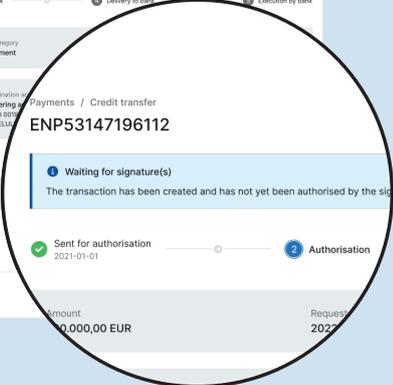
03.
GET AN OVERVIEW OF THE BALANCES OF ALL YOUR BANK ACCOUNTS

04.
SCREEN NAMES & MANAGE RESULTS

HOW
DOES IT WORK?

A SAAS-HOSTED PLATFORM

ENPAY is operated by Finologee in a software-as-a-service mode, as a platform hosted in Luxembourg that covers all payment process operations and execution stages, while providing a virtually unlimited access to banks across the world through the SWIFT network. Through this single-entry product, fund managers can streamline their processes by automating payment order messaging, transaction validation and reporting.

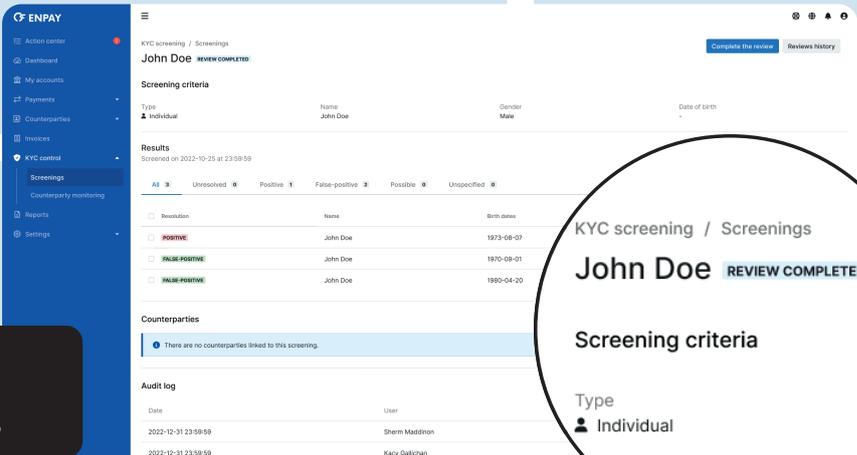### WEB INTERFACES OR API ENDPOINTS

User authentication, workflows and transaction signatures are handled on the ENPAY platform, either through secure and easy-to-use web interfaces (for manual entry or batch upload) or ENPAY's API endpoints (for system interconnection), without the need for additional authentication/signatures using the banks' mechanisms.

ROLE-BASED ACCESS

The platform encompasses adaptable role-based access where authorised users can carry out all their tasks such as single or batch payments and counterparty management.

A DIRECT ACCESS TO THE SWIFT NETWORK

ENPAY relies on a direct connection to the SWIFT financial messaging network (with its own BIC code) through which most bank accounts can be connected to the platform with no additional technical impact on the banks' side.

TAILORED TO YOUR NEEDS

When defining the scope and the setup of an ENPAY implementation project, Finologee works closely with its clients to define user roles and permissions that accurately reflect their organisation and approval rights.

USE CASES OF ROLE-BASED ACCESS IN THE ENPAY SYSTEM THAT CAN BE ADAPTED TO YOUR NEEDS

ACCOUNTANT, ADMINISTRATIVE ASSISTANT, MIDDLE OFFICER

Feature access:
- Counterparties creation
- Single payment entry
- Batch job upload
- Audit log
- Reporting
- Dashboard access

HEAD OF ACCOUNTING, CHIEF FINANCIAL OFFICER, COMPLIANCE OFFICER...

Feature access:
- View all actions initiated via ENPAY
- Counterparties management (including blacklisted IBAN management)
- Payment creation
- Audit log
- Reporting
- Dashboard access

### 1ST AND 2ND SIGNATORY: SIGNATORIES MANAGEMENT (C-LEVEL, GPs, LPs...)

Counterparties rejection/approval
- Payments authorisation according to internally defined rules
- Amounts and ordering accounts
- Dashboard access

WHAT ARE

THE PLATFORM HIGHLIGHTS?

01 MULTI-BANK ACCOUNT CONNECTIVITY

Optimise your payment processes by not having to connect manually to several remote banking interfaces.
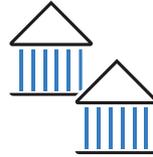
02 COMPREHENSIVE OVERVIEW OF ALL INCOMING & OUTGOING PAYMENTS

Improve your supervision capacity with an all-encompassing visualisation of all transactions.

03 STREAMLINED PAYMENT VALIDATION WORKFLOWS

Increase efficiency by connecting various stakeholders involved in the payment approval process with multi-level user access, rights management & notifications.
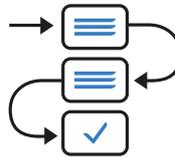
04 FRAUD PREVENTION AND RISK MANAGEMENT FEATURES & REPORTING

Streamline payment process-related regulatory challenges by retrieving a full audit trail, detailed payment status reporting & more.

05 FIRST-CLASS USER EXPERIENCE & AUTOMATION

Modern, fast, secure, and easy-to-use interfaces that require little or no training. Get a quick overview - depending on the role - of what steps are required on your side to complete transactions.

WHAT ARE THE MAIN
FEATURES?

01 IN & OUTGOING PAYMENTS

02 MULTI-BANK ACCOUNT AGGREGATION

03 STANDING ORDERS

04 ADVANCED COUNTERPARTY/
BENEFICIARY MANAGEMENT

05 PEPPOL ACCESS POINT MODULE

06 VERSATILE WORKFLOW MANAGEMENT

07 MULTI-LEVEL USER ACCESS &
RIGHTS MANAGEMENT

08 MULTI-FACTOR AUTHENTICATION (MFA)
& E-SIGNATURES

09 API END-POINT

10 FULL AUDIT TRAILS

11 COUNTERPARTY RISK LEVEL MANAGEMENT

12 RULE-BASED EMAIL &
SMS NOTIFICATION SYSTEM

13 CHARTS, FLOWS & CASH MANAGEMENT

14 ROLE-BASED DASHBOARD &
ACTION CENTRE INTERFACES

15 KYC/AML SCREENING & MONITORING

16 DOCUMENT ATTACHMENTS TO TRANSACTIONS
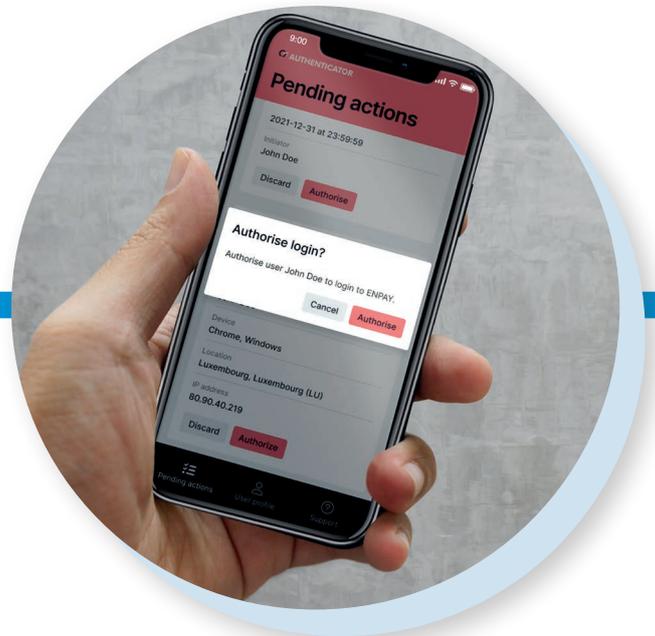
Check page 16 to discover more on FinologeeAuthenticator

Learn more about our risk management features embedded
in the payments platform on page 20

HOW
DOES ENPAY
HELP YOU?

LET'S HAVE A LOOK AT THE SCREENS

ACTION CENTER

The action center provides a useful overview of all actions pending in relation to credit transfers, counterparties, and KYC screenings. Users get a fast-track access to the actions that are relevant to them.
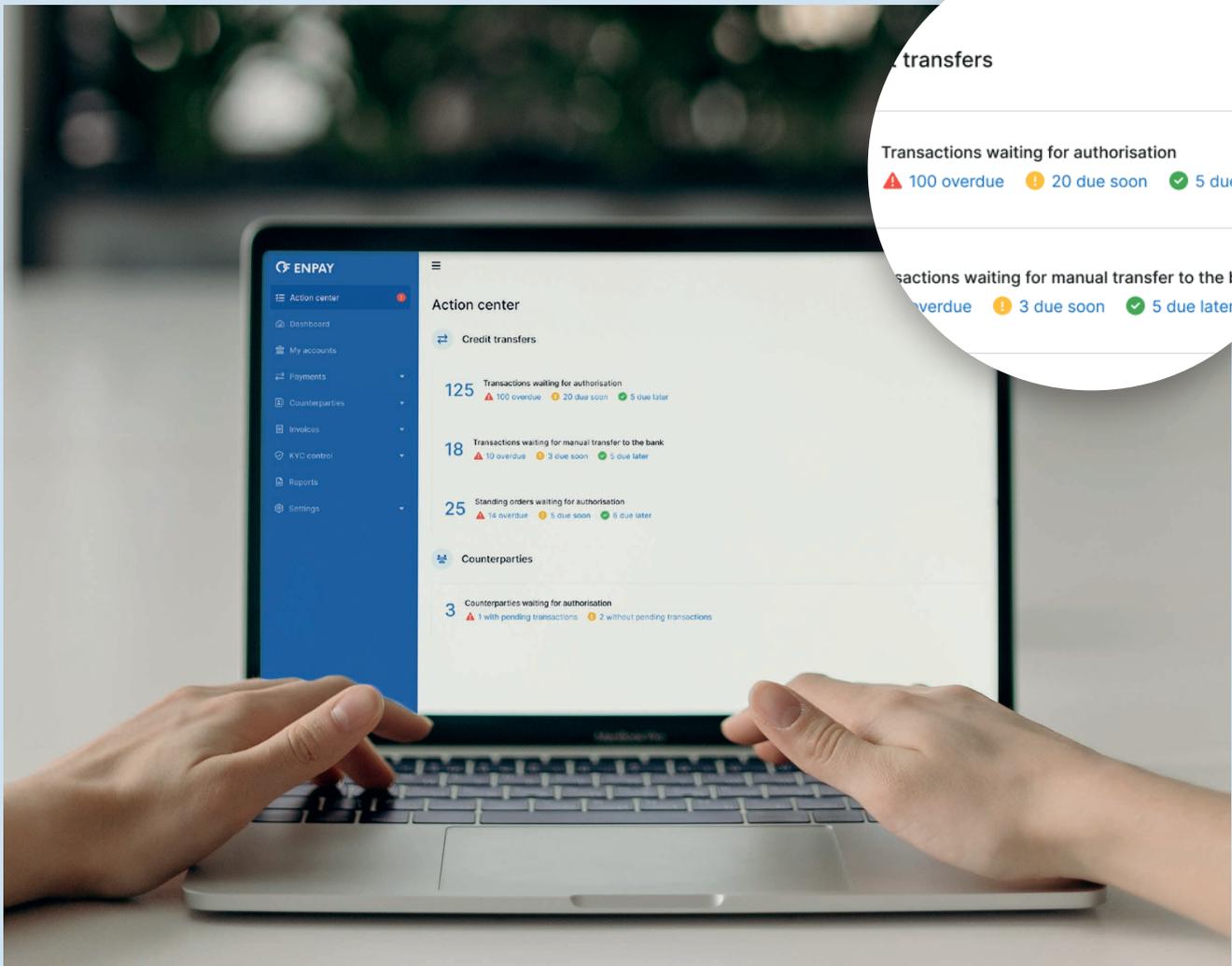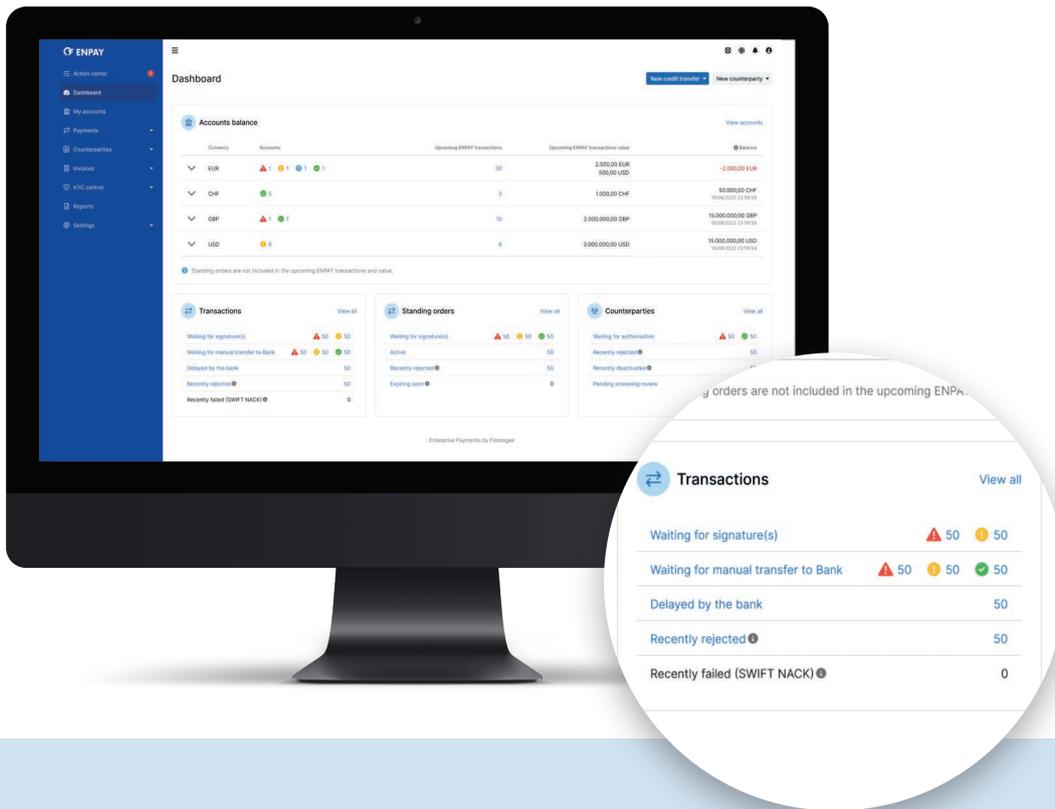
OVERVIEW DASHBOARD

The dashboard enables quick data access and visualisation of payment activities on the platform. The information is customised for each user according to their role. It provides a clear overview of own and other pending actions as well as rejected and not executed transactions. It includes shortcuts to access the main views and to perform quick actions.
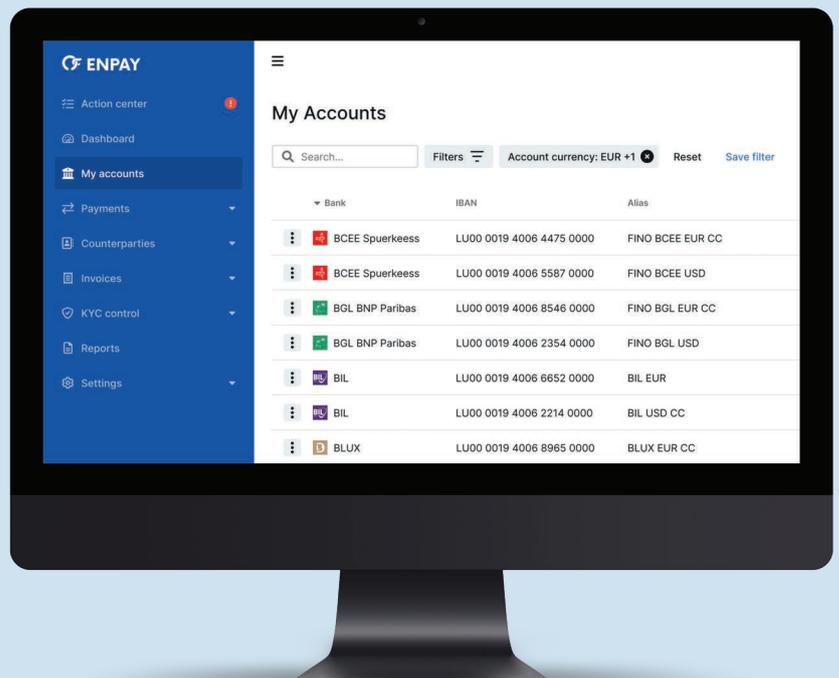
MY ACCOUNTS

The navigation bar item My Accounts is the go-to place to get an overview of the balances of all bank accounts: here you can view balances per account over time, access all incoming and outgoing transactions and retrieve account statements.
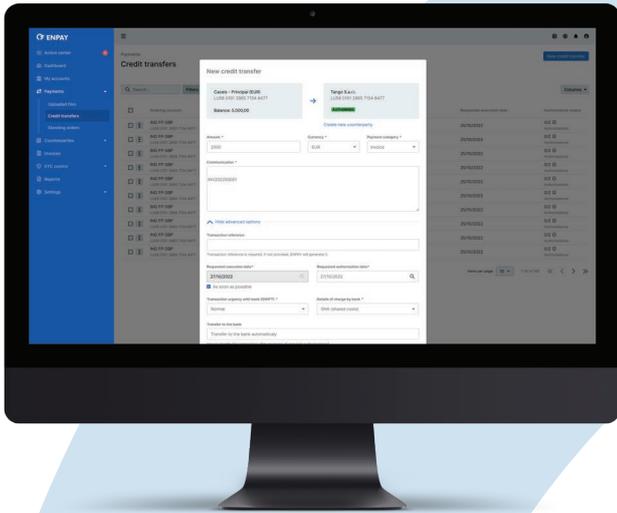
PAYMENTS

01. Setting up new credit transfers is a simple process: the user selects the ordering account and the counterparty here. If the counterparty is not in the system yet, it can also be created at this moment. Once all transaction details have been entered, users receive a transaction overview.

02. This page provides an overview of all transactions that have been entered into the system. Users can search for individual transactions by specific elements such as status, counterparty or amount. An advanced search feature is also available to quickly find past transactions in the system.
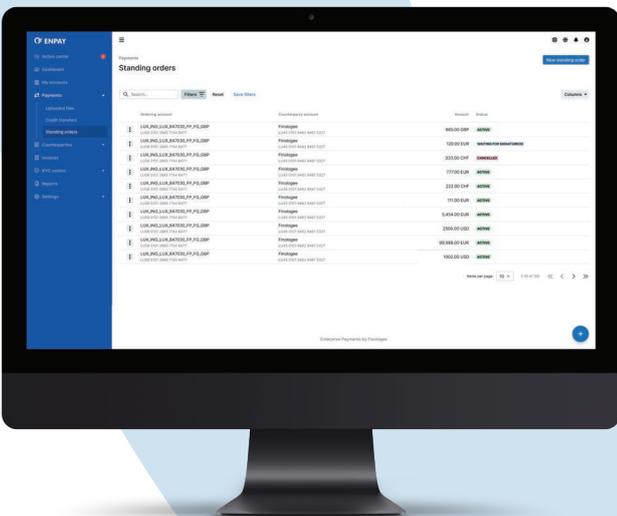
03. The ENPAY platform allows clients to manage their standing orders with any bank. It provides an instant overview of the status and details of orders and allows them to be modified with just one click. On top of that, it encompasses dedicated standing order authorisation workflows.

COUNTERPARTY & ADVANCED RISK MANAGEMENT

01. Counterparties are created in the system and may be subject to an authorisation process by other users/groups. ENPAY also provides a 'blacklisted IBAN' feature to lower the risk of fraud.
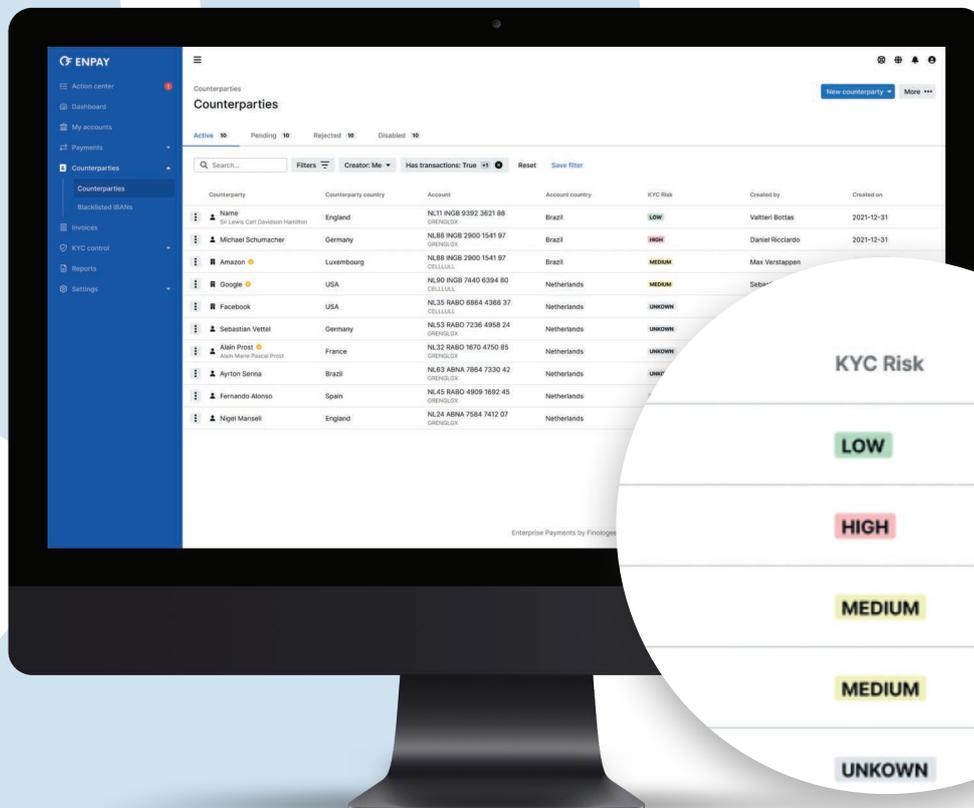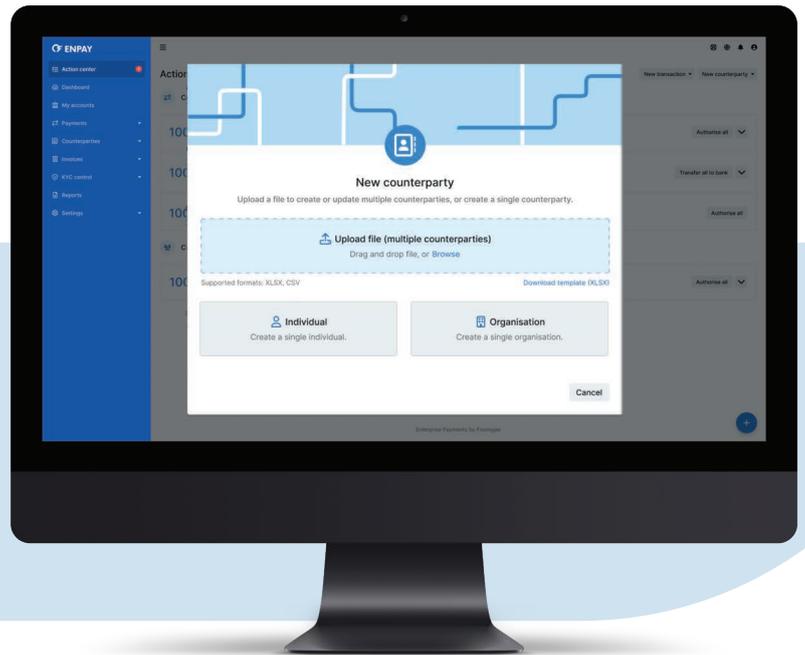
02. Mitigate risk and ensure AML/CFT compliance by easily assigning risk levels to counterparties and defining workflows per level. ENPAY enables real-time collaboration between accounting and compliance, giving the user a clear and efficient overview of risk history, its tracing and related comments, and documents.

REPORTS

The ENPAY reporting tool allows any user, based on its role (e.g., accountants, auditors or compliance teams) to generate and export payment reports. The product includes custom reports and account statements with filtering options (e.g., date range, accounts ...) that can be downloaded as PDF, XLS or MT940 files.
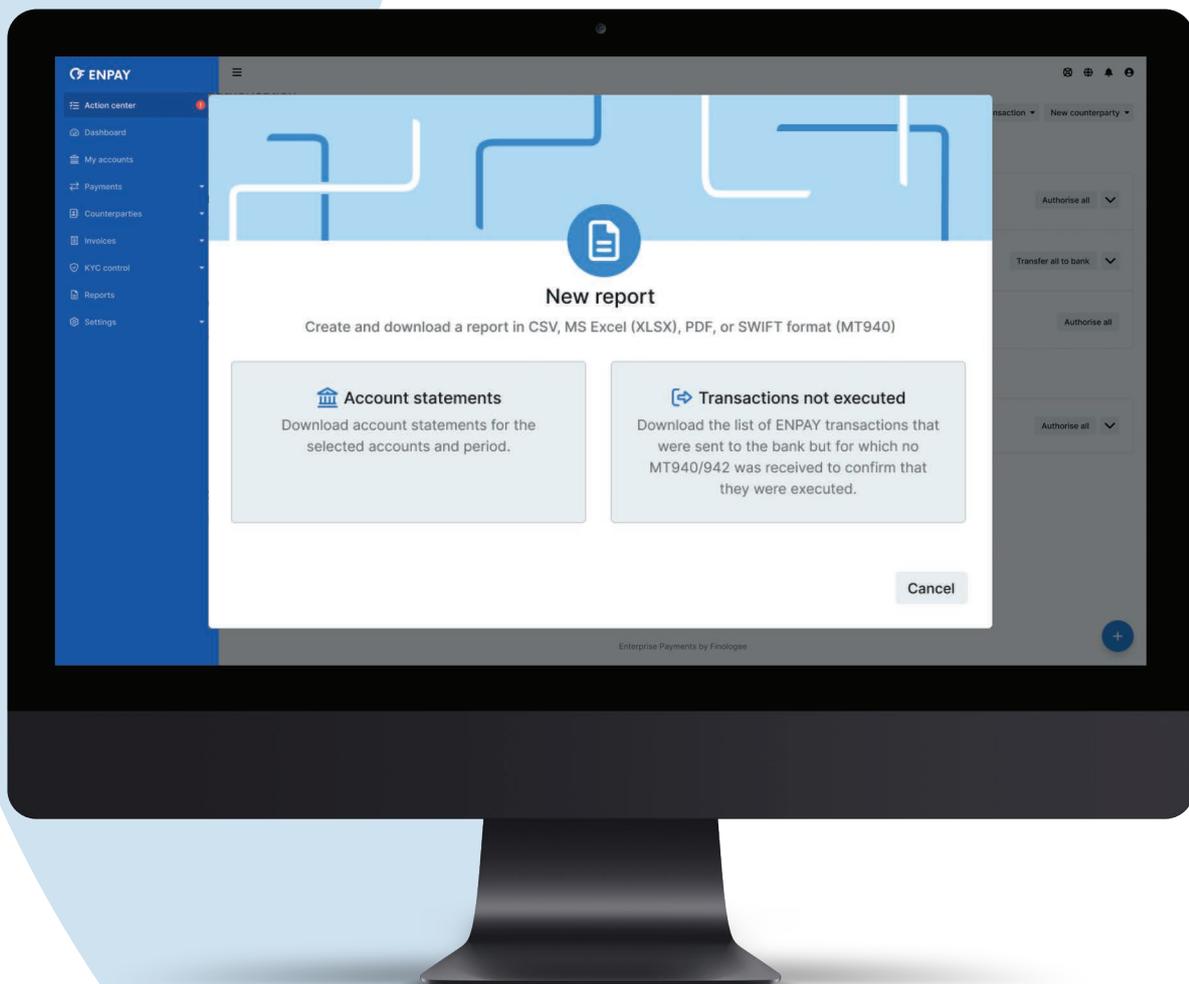
AUTHENTICATION

The ENPAY platform provides a high level of flexibility for authentication and electronic signing of transactions (and approving counterparties): clients can choose to rely on Finologee's own corporate authentication/ e-signature framework, Luxtrust certificates and clients' own corporate authentication frameworks.
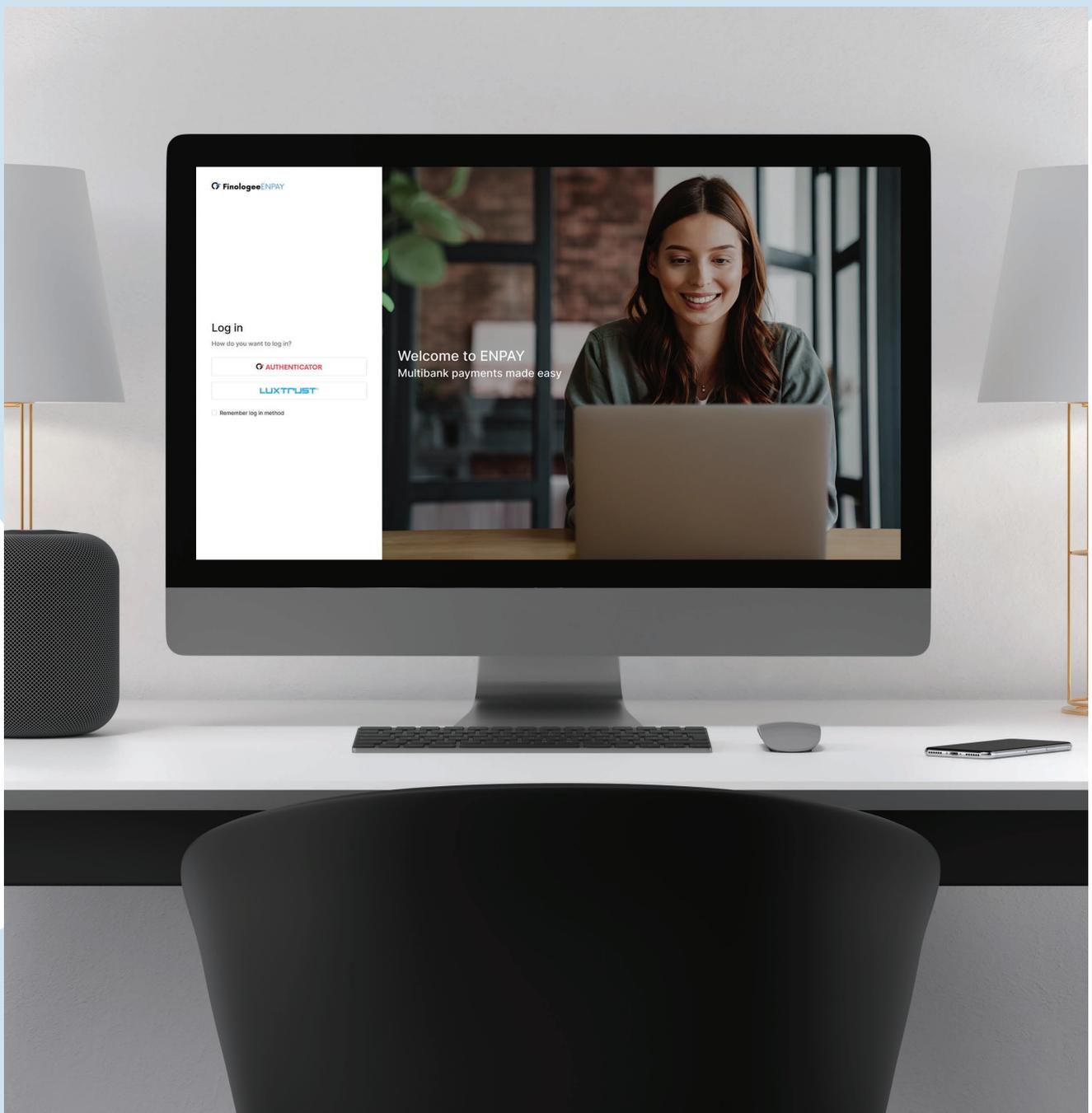
DISCOVER
THE LATEST PRODUCT FEATURES

Multi-factor authentication with FinologeeAuthenticator

Multi-bank account connectivity is a challenge that affects most businesses and financial industry players. ENPAY – as a **comprehensive payment platform encompassing access to all bank accounts** - is by default many times more **time and cost-efficient** than selecting, implementing, and using different tools and services from different banks or providers.

01

02
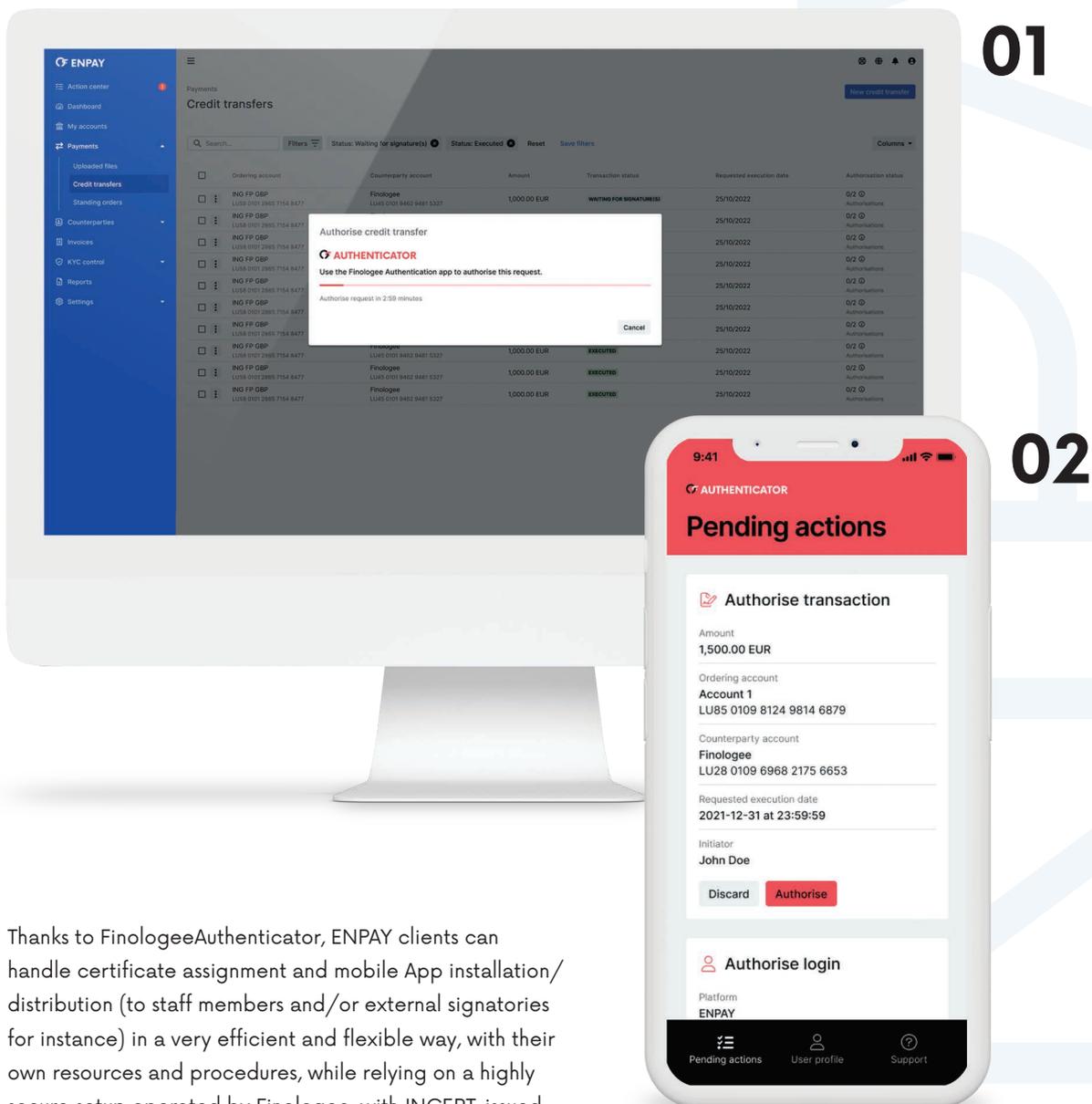
Thanks to FinologeeAuthenticator, ENPAY clients can handle certificate assignment and mobile App installation/distribution (to staff members and/or external signatories for instance) in a very efficient and flexible way, with their own resources and procedures, while relying on a highly secure setup operated by Finologee, with INCERT-issued certificates at the core of the framework.

Finologee's Authenticator stack also provides several advanced features that streamline daily operations, such as a user management system available through one or more secure administrator accounts, with 4 eyes principle/approval workflows, as well as user audits with export features that are very useful with regards IT security and compliance requirements.

Connection to the international PEPPOL network

Finologee's Peppol Access Point allows for the exchange of invoices and documents with public authorities and institutions, as well as for business-to-business and business-to-consumer workflows. The aim is to enable companies to use the Peppol network to transmit messages such as invoices and orders more efficiently and securely.

Compliant invoicing flows in a few steps

1

Upload Invoice
(CSV, JSON, XML, etc...)

2

Request to pay

3

Invoice

Track status of invoice
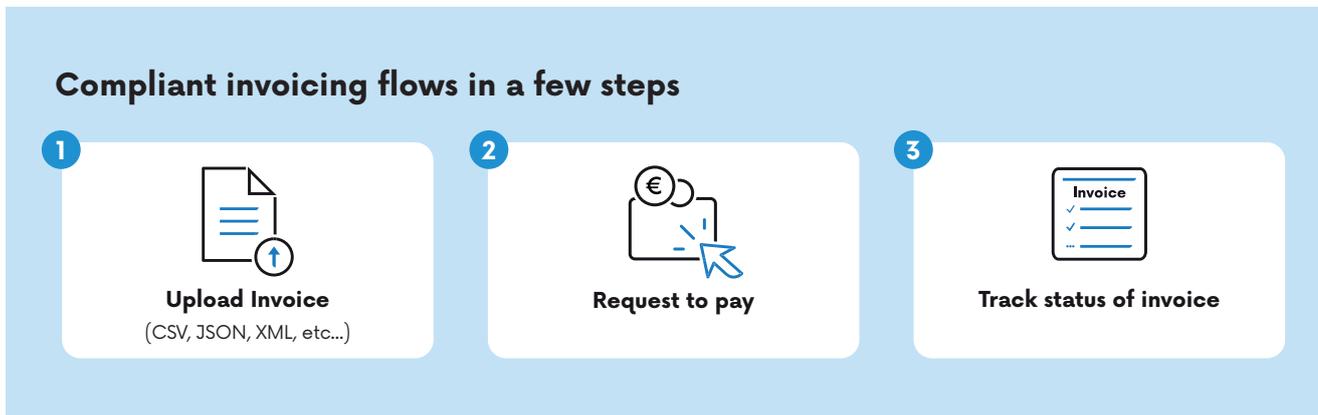
PEPPOL
CASE STUDY

LALUX IMPLEMENTS PEPPOL E-INVOICING WITH FINOLOGEEENPAY

lalux
ASSURANCES

The well-known Luxembourg insurance company LALUX is using the Finologee Peppol Access Point to send electronic invoices to the Luxembourg Government, public institutions, and municipalities. Finologee provides a Peppol access point integrated within FinologeeENPAY, its professional payments and multi-bank account access management platform. ENPAY is operated in a Software-as-a-Service (SaaS) mode and is accessible through a secure API endpoint. Prior to automating and streamlining its invoicing process, LALUX had to manually fill their invoices using the template provided by the Luxembourg Government.

THE CHALLENGE
Following the publication of the law from 14 December 2021 regarding electronic invoicing in the Official Journal, large businesses are now obliged to transmit their invoices electronically to the Luxembourg Government in the

context of public procurement, supplier, and concession contracts. For this purpose, they will mainly use the CTIE Peppol Access Point. By 18 October 2022 and 18 March 2023 respectively, Business-to-Government e-Invoicing becomes mandatory for medium-sized and small businesses as well.

Formerly, LALUX used to convert its standard invoices manually. This was very time-consuming and labour-intensive. Therefore, the Luxembourg insurer was looking for an easy-to-use tool to send its invoices to public authorities in Luxembourg.

THE SOLUTION
Finologee's Peppol Access Point can be used for exchanging documents with public authorities and institutions, as well as for business-to-business and business-to-consumer workflows. The aim is to enable companies to use the Peppol network to transmit messages such as invoices and orders more efficiently and securely. The Peppol network is worldwide, meaning that companies can send and receive e-invoices internationally. We asked Vincent Arnal, CIO at Lalux, on why they chose to implement Finologee's ENPAY Peppol module and what benefits they see.

WHY DID YOU CHOOSE TO IMPLEMENT FINOLOGEE'S ENPAY PEPPOL MODULE?
"In view of the new law – which led us to rethink our internal process regarding the invoices that we send to the government – we were looking for an access point to get

connected to the Peppol network. Finologee, being one of the only Luxembourg Certified Peppol Service Providers, offered what we were looking for. They were very open to explore how we could best integrate the Peppol module according to our specific needs. The decision to work with them was easy as we already knew Finologee and their team."

HOW WOULD YOU DESCRIBE THE COOPERATION WITH FINOLOGEE?

"The cooperation and communication with the Finologee team went smoothly. In a series of workshops, we analysed together how we could convert the existing data that we had exported from our systems into the required Peppol document format (UBL). For this, Finologee developed a very efficient approach. Also afterwards, they were always ready to help us in any way they could."

THE OUTCOME

Finologee has developed a customised approach to best meet the company's needs. This includes accessing the network, converting the files from the format they use and archiving the invoices. By connecting to the network early,

LALUX is a pioneer and is preparing for what Peppol has to offer when many players will be connected. A future evolution may be to send B2B invoices and add capabilities to receive invoices via the Peppol channel.

WHAT CONCRETE ADVANTAGES CAN YOU NAME FOR THE USE OF THE ENPAY MODULE?

"Finologee is a regulated company that operates as a PSF and is fully audited – for us this is a guarantee of reliability and security, as it offers legal archiving in a regulatory compliant environment and provides all necessary documentation. Besides, supplier onboarding and due diligence was straightforward with the company."

ABOUT LALUX

LALUX Assurances is one of the historic leaders in the Luxembourg insurance market. The insurance company offers a variety of services, such as, automotive, housing, health and accident, civil liability, as well as life & death insurance. With its deep roots in Luxembourg's economic and social fabric as one of the Grand Duchy's largest employers, the "La Luxembourgeoise" currently employs about 500 staff in the Grand Duchy.
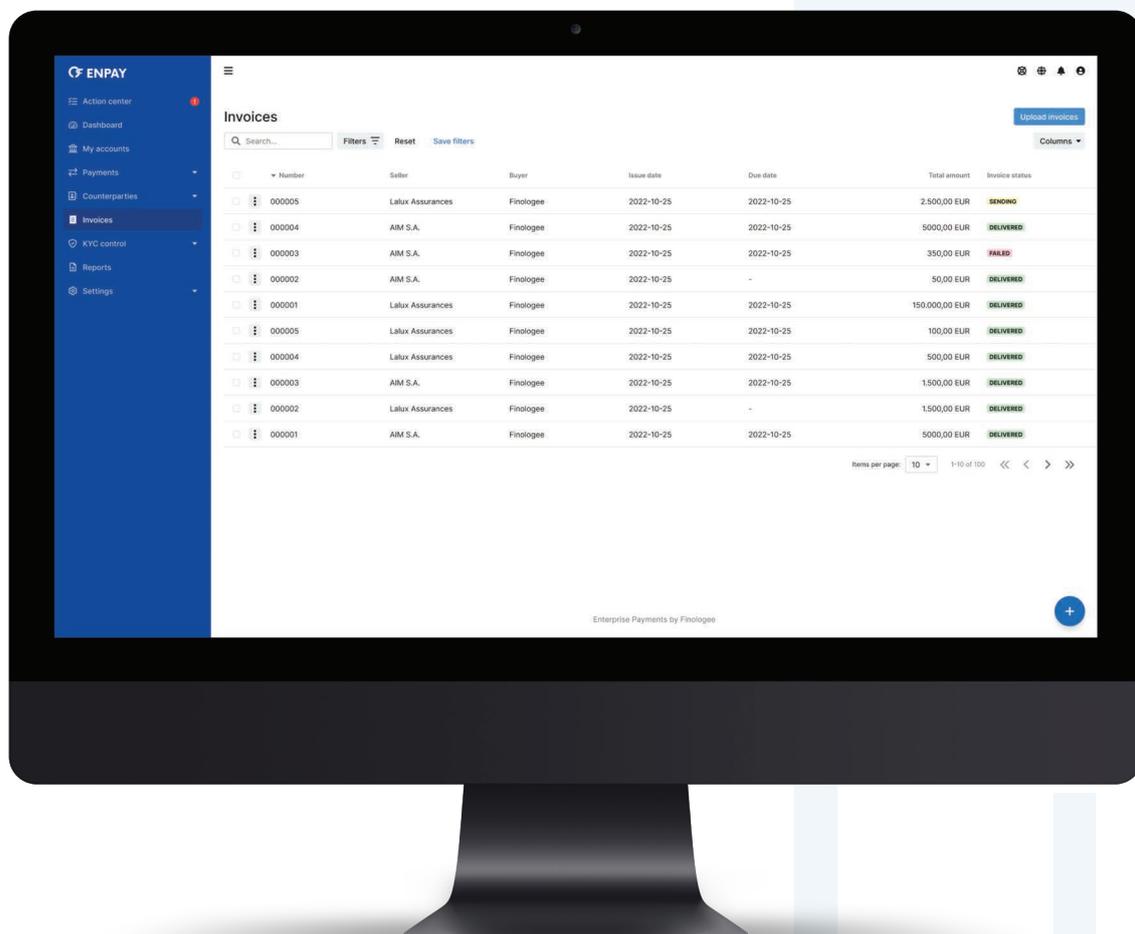
RISK
MANAGEMENT FOCUS
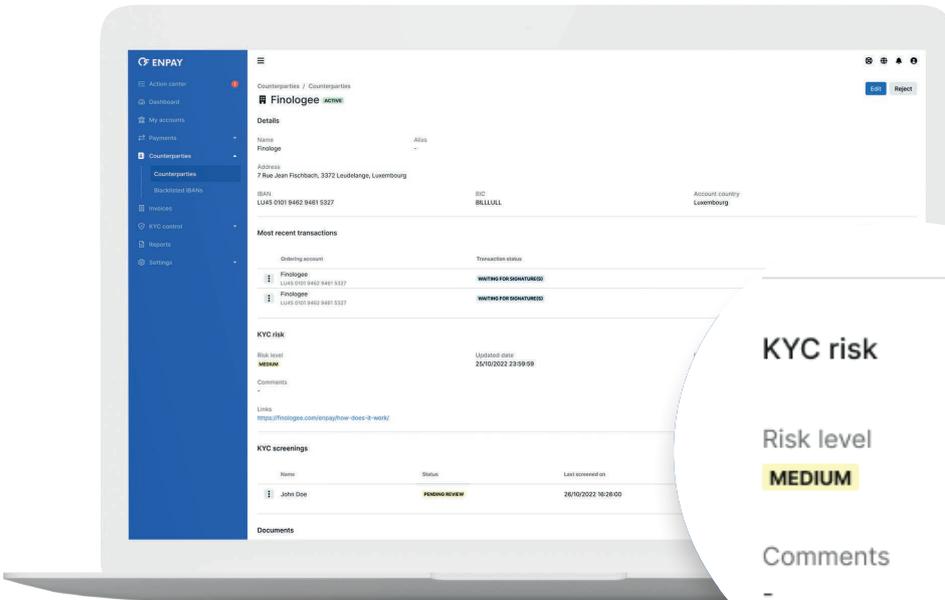
Counterparty risk management

Mitigate risk and ensure AML/CFT compliance by easily assigning risk levels to counterparties and defining workflows per level.
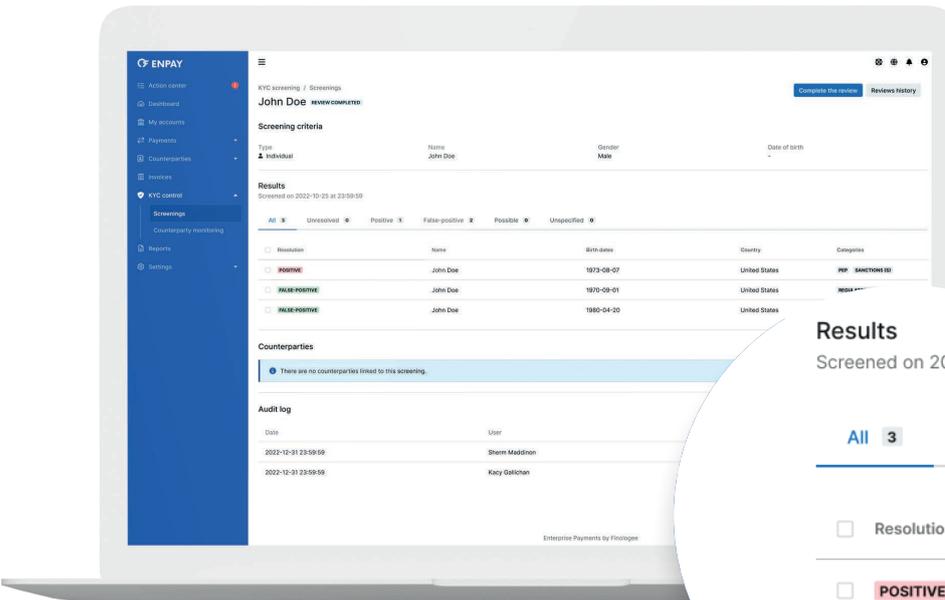
KYC name screening using blacklist/ sanction list providers

ENPAY enables user-friendly KYC name screening with the option of zero-footprint scanning. View matches across relevant sanction lists, law enforcement watchlists, lists of PEP and their resolution status.
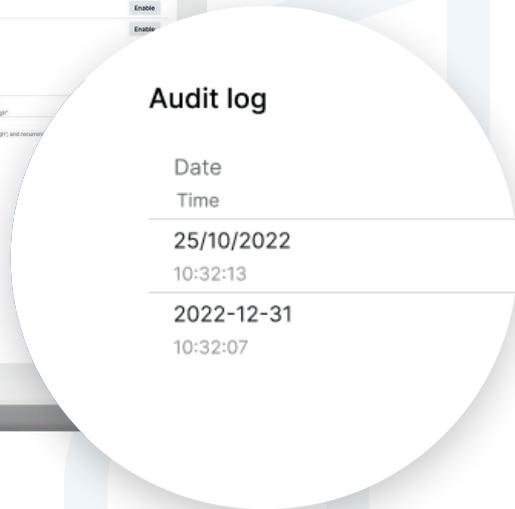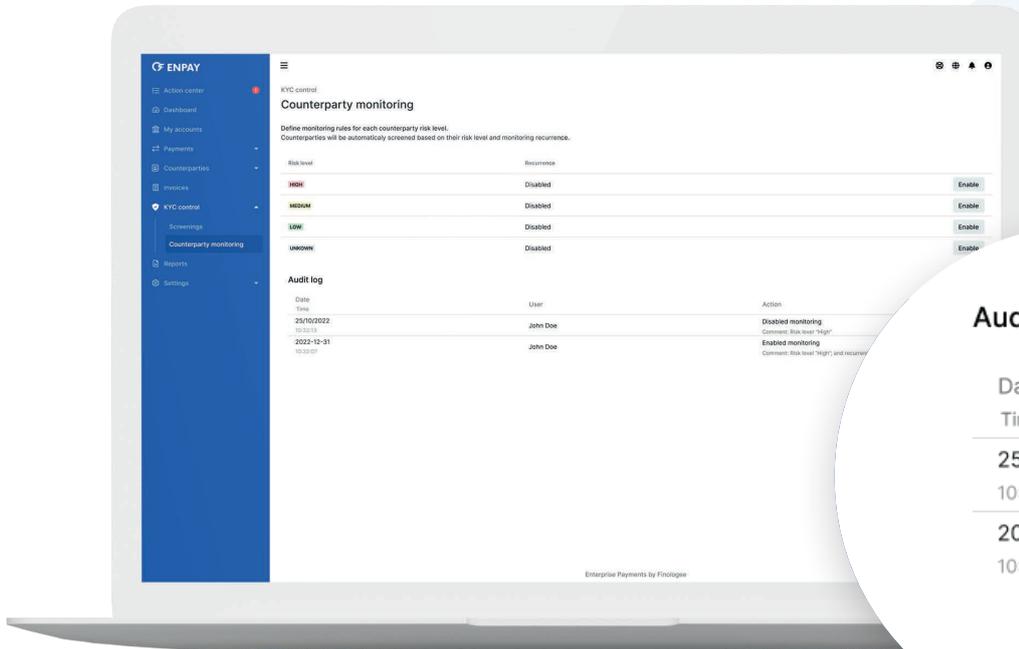
Link screenings to one or more existing counterparties and retrieve the corresponding **audit trail** with detailed signature steps, bank process steps, confirmation or error reports.
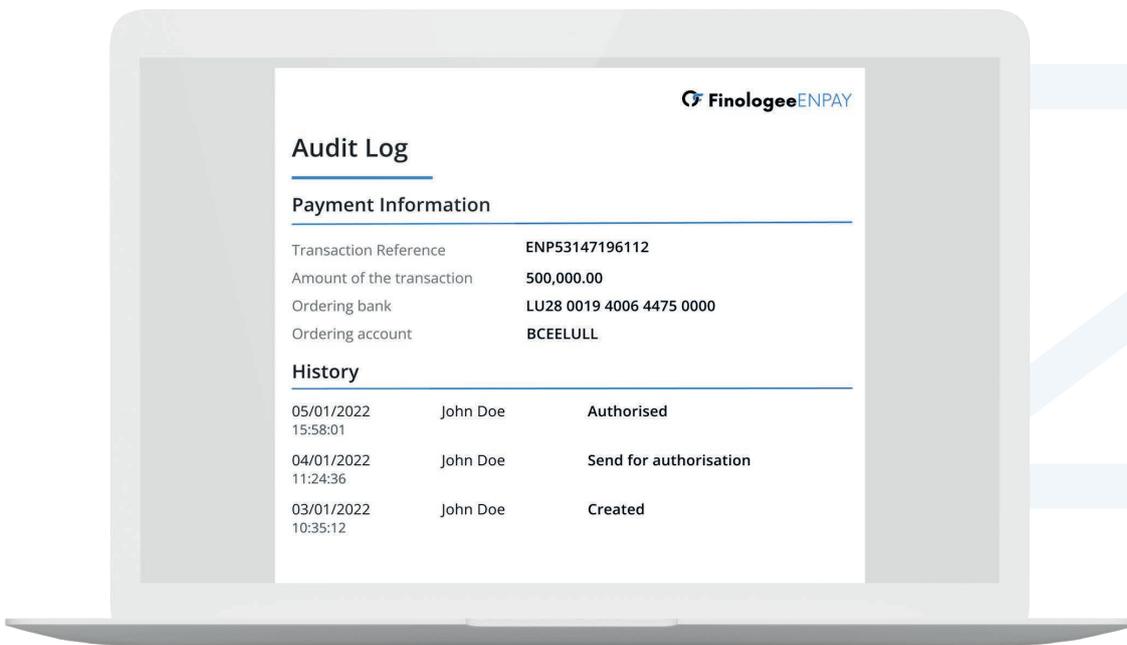
Audit & transparency features
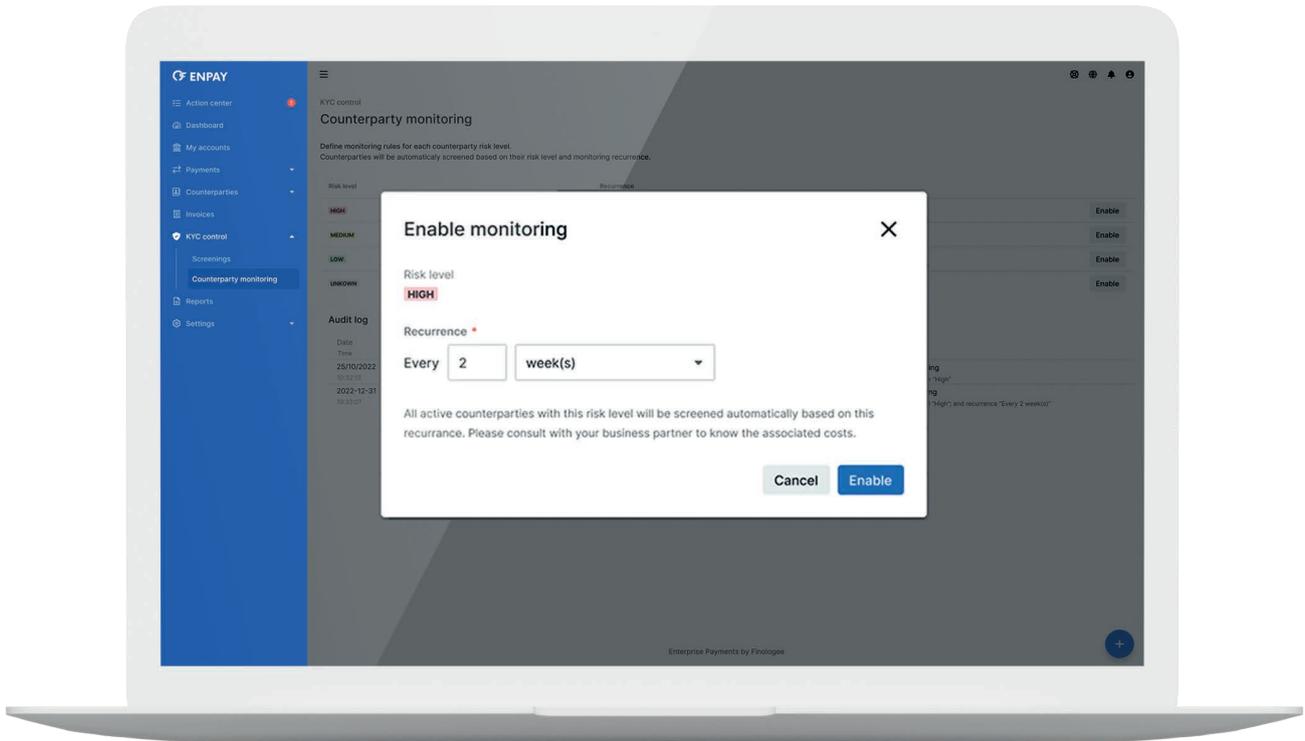
Counterparty monitoring

Define monitoring rules for each counterparty risk level. Counterparties are automatically monitored based on their risk level and monitoring recurrence **rules matching your AML/CFT policies.**

STREAMLINE PAYMENT PROCESS

REGULATORY CHALLENGES WITH ENPAY *3 February 2022*

ENPAY has been designed to enable financial industry and institutional players to enhance their payments processes. Beyond operational efficiency and true to Finologee's identity as a RegTech and a regulated Professional of the Financial Sector (PFS), ENPAY has been developed with **regulatory compliance at its core** all the way from the choice to use ENPAY, to the execution of payments, to accounts reconciliation and reporting obligations after the payment process. In this article, we will outline these steps in detail and point towards the respective compliance aspects that are particularly important for regulated entities.

Find out how ENPAY can provide secure and reliable answers in a largely "tick the box" approach to compliance – in 3 steps:

STEP 1
CHOOSING ENPAY – MEETING ICT OUTSOURCING AND SECURITY OBLIGATIONS

01. COMPLIANT OUTSOURCING IN LINE WITH CAA AND CSSF EXPECTATIONS

Feedback from our regulated clients is that one of the key legal challenges in selecting an external provider (especially one that will assist with sensitive business processes such as payments flows) is to ensure full compliance with the wide array of regulatory obligations relating to outsourcing. ENPAY and the underlying platform on which it relies aim to **facilitate the outsourcing compliance process** in several ways:

• ENPAY is designed to provide the **technical tools** to support clients with their payments processes whilst enabling them to **retain control and flexibility over process specifications** (e.g. payments validation requirements, authentication and signature mechanisms, etc.). This should facilitate compliance with regulatory principles limiting the ability to outsource core functions and requiring regulated entities to retain control over business processes.

• **The terms and conditions applicable to ENPAY meet Luxembourg and EU outsourcing requirements**, notably: Circular **CSSF 12/552** on Central Administration, Internal Governance and Risk Management; the **EBA Guidelines on Outsourcing** Arrangements; the Law of 7 December 2015 on the insurance sector and Article 274 of Commission Delegated Regulation (EU) 2015/35 of October 2015 supplementing the **Solvency II**.

Did you know? *As a Support PFS subject to CSSF supervision, Finologee is itself subject to equivalent outsourcing obligations (notably through Circular CSSF 17/656 which mirrors banks' outsourcing obligations in Circular CSSF 12/552), ensuring that regulatory requirements are met throughout the outsourcing chain.*
Finologee is also subject to identical professional secrecy obligations as financial institutions and insurance companies pursuant to article 41 of the law of 5 April 1993 on the Financial Sector.

• ENPAY is **hosted in Luxembourg with EBRC**, which is **also a Support PFS**. EBRC is the number one player in Luxembourg market in its field and has a redundant setup with **three certified Tier IV data centers**. It operates back-to-back

with Finologee's ISO27001 and SLA commitments, providing Finologee with a dedicated platform designed to be **fully compliant with IT outsourcing requirements** imposed on Finologee pursuant to Circular CSSF 17/656.

02. BANK-GRADE ICT AND SECURITY RISK MANAGEMENT

Information and communication technology (ICT) and security risk management obligations, including in respect of the use of suppliers, have also multiplied in recent years, notably with the publication by the CSSF of **Circular CSSF 20/750** on Requirements regarding information and communication technology (ICT) and security risk management in August 2020. This trend is likely to continue, with the approaching implementation of the Digital Operational Resilience Act, known as **"DORA"**, which will create a harmonised framework of rules that all institutions supervised by either the EBA, the EIOPA or ESMA will need to follow relating to operational resilience.

Finologee aims to enable regulated players to apply a largely **"tick the box" approach to compliance** with these obligations when selecting it as their ICT outsourcing provider:

• As a Support PFS, Finologee is also **directly subject to the obligations of CSSF 20/750** (which applies to all entities within the CSSF's perimeter of supervision). In addition, it applies state-of-the-art security standards and is **ISO/IEC 27001** certified. These elements guarantee bank-grade compliance with ICT and security risk management obligations, which in practical terms, **greatly facilitates assessment and monitoring** for our clients since there is a strong parallel between our respective security commitments.

• **ENPAY relies on professional channels such as SWIFT**, the world's leading provider of secure financial messaging services, to interact with account banks to ensure best-in-class security standards in the transmission of data. Since SWIFT is a professional network made up of financial institutions and assimilated entities, Finologee's eligibility to participate stems from the fact that it is a regulated entity which satisfactorily meets SWIFT's membership criterion. Finologee is subject to **regular audits from SWIFT** to ensure that its SWIFT-related infrastructure continuously meets SWIFT's security criteria.

*Finologee's expertise has been recognised by the Luxembourg IT community by **awarding Finologee "ICT Outsourcing Services Provider of the Year" at the 15th edition of Gala IT One.***

STEP 2
– CARRYING OUT PAYMENTS – FACILITATING COMPLIANCE WITH RISK MANAGEMENT OBLIGATIONS

01. FRAUD PREVENTION

For regulated companies, ensuring that there are robust accounting processes in place is part of the central administration requirements set out in applicable texts (notably: Circular CSSF 12/552, the Law of 5 April 1993 on the Financial Sector, and the Law of 7 December 2015 on the Insurance Sector).

A strong focus of these requirements is on the **"integrity" of the accounting organisation**. The CSSF, for instance, specifies in Circular 12/552 that accounting procedures must be defined and implemented to "ensure compliance with the principle of integrity to avoid, in particular, that the accounting system is used for fraudulent purposes" (Section 2.5.3.2. on the financial and accounting function).

International audit norms used by external auditors for reviewing regulated companies' accounts also include detailed obligations relating to fraud detection in financial statements (see particularly ISA 240). This includes the misappropriation of assets, often through employee fraud (e.g. embezzling receipts of causing the entity to pay for fictitious goods/services). The ISA 240 norms recognise that misappropriation of assets may occur due to inadequate internal control, including an "inadequate system of authorisation and approval of transactions". This means that financial institutions and insurance companies have not only an operational incentive, but also a legal obligation, to ensure that the risk of fraud in their accounts is well managed.

ENPAY may help by enabling companies to implement **sophisticated order validation workflows** involving **different departments** (for example, requiring sign off from the compliance department for all payments over a certain amount). The rules underlying the workflows are fully customisable to reflect clients' **internal policies and processes** and can also easily evolve over time along with **changes in regulation or the level of risk.** Integrity is ensured by relying on **secure authentication and signature mechanisms**, using LuxTrust, FinologeeAuthenticator or relying on a client's own stack.

In addition, ENPAY keeps a detailed **record of user profiles** so that permissions granted to an employee/member of management at any given time are easily visible. This

may also be used to streamline responses to queries from auditors/regulators, as it is for instance possible to **export a list of authorised users and provide it** directly to the requesting party (e.g. an auditor).

02. COUNTERPARTIES MANAGEMENT & AML/CFT REQUIREMENTS

Another important aspect of payment workflows is the management of counterparties and in particular, the **handling of money laundering and terrorism financing risks.** CAA Regulation 20/03 and CSSF Regulation 12-02 (as amended by CSSF Regulation 20-05), in this respect, both make it clear that the audit of annual accounts of insurance companies by the approved statutory auditor should include the compliance with AML/CFT requirements. ENPAY is a powerful tool to increase AML/CFT compliance in counterparties and transaction management, by:

• Ensuring that payments are **made only to pre-approved beneficiaries** saved in the ENPAY interface with automated controls on each transaction/counterparty creation or modification (applying an adequate validation workflow and checks against any blacklisted IBANs);

• Enabling **bidimensional visibility on the relationship with any given counterparty**, by being able to view both outgoing and incoming payments in a consolidated view;

• Setting up automated checks set up to verify that payments are systematically being made to, and coming in from, the same account initially associated to a counterparty;

• Creating **payment thresholds** and differing **validation processes** based on criteria such as AML/CFT risk of a given type of transaction or counterparty.

STEP 3
– AFTER THE PAYMENT: ACCOUNTS RECONCILIATION AND REPORTING OBLIGATIONS

In close connection with reducing of the risk of fraud, it is also important for companies to have an accurate, real-time overview of outgoing and incoming payments. This is not only an operational necessity, but also required to comply with **accounting obligations** (e.g. to reconcile accounts and accounting entries) as well as with **reporting and audit obligations.**

Such reporting and audit obligations include, of course, the preparation of annual accounts and their review both internally and by an external auditor. Through ENPAY, Investment firms or insurance companies for instance that are subject to the Capital Requirements Regulation (575/2013) and Solvency II (Directive 2009/138/EC), can rely on **consistent source data including visibility on underlying flows** which is essential in this context, given the careful financial management and analysis required to comply with the obligations stemming from these texts. ENPAY, through its multi-bank connectivity, allows all payment information to be available on a single platform, whilst ensuring the integrity of the displayed information through robust processes. The platform can be used to **export audit logs** (through embedded export pdf functionalities) and generate **time-stamped consolidated statements** (using electronically signed/e-sealed documents). These reporting functionalities can be customised: For example, it is possible to filter reporting by counterparty in order to obtain a **bidimensional counterparty view** of outgoing and incoming payments, which can save precious time in accounting processes. ENPAY also integrates sophisticated **reporting and analytics** including in-detail insights on transactions. These features, which provide real-time qualitative data that is easy to exploit, may thus be particularly helpful with **information reconciliation** in the context of internal and external control missions and in preparing financial reporting. The consolidated reporting and data export functions can also be used to **streamline responses to audit requests.**

PARTNERS
& CONNECTIVITY

Banks connectivity provider

Supported by

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Authentication & transaction e-signature

Certificate provider for FinologeeAuthenticator

LUXTRUST®
Enabling a digital world

INCERT
Because it's always a matter of security

DID YOU KNOW?
ENPAY IS OPTIMIZED FOR LUXEMBOURG-BASED ENTITIES
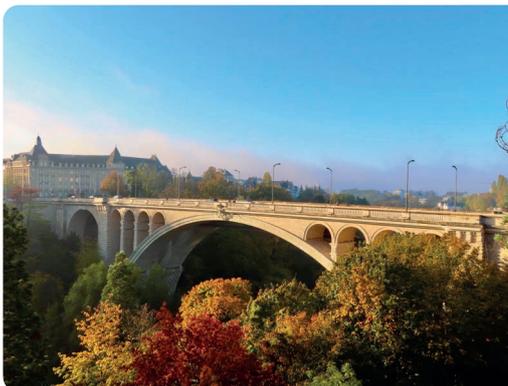
- Hosted and operated in SaaS setup in Luxembourg – no on-premise installation required, but API integration possible

- Straightforward compliance with EU & Luxembourg outsourcing regulations through Finologee's "Support PFS" licence

- ISO 27001:2013 certified

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:

SOCIETE GENERALE · PICTET 1805 · Goldman Sachs · CA INDOSUEZ WEALTH MANAGEMENT · 支 Alipay · BGL BNP PARIBAS

CA CRÉDIT AGRICOLE LIFE INSURANCE · Foyer · SwissLife · UniCredit International Luxembourg · BIL 1856 · 中国建设银行(欧洲)有限公司 China Construction Bank (Europe) S.A.

Raiffeisen · POST LUXEMBOURG · Deka · AG2R LA MONDIALE · EDB · e · ∞ payconiq

ACL · AZQORE PARTNERS FOR TOMORROW'S WEALTH MANAGERS · bradesco europa · lalux ASSURANCES · ALPHA BANK · BANQUE HAVILLAND

(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

mpulse.

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.

GET
IN TOUCH

ENPAY EMPOWERS FINANCIAL INDUSTRY PLAYERS AND INSTITUTIONS TO STREAMLINE ALL THEIR PAYMENT AND REPORTING PROCESSES.

WWW.FINOLOGEE.COM

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