Electronic Money Institution Reference Guide

June 2024

About this document

This document provides information regarding the Electronic Money Institution (EMI) within the meaning of EU legislation.

The document is designed to be read in conjunction with information provided by the European Banking Authority (EBA) and the Central Bank of Ireland (CBI) to which reference is made in this document, and in conjunction with the Payment Services Directive (PSD2) from which national legislation pertaining to EMIs is derived.

Links to the PSD2 and to relevant sections of the EBA and CBI websites are included for reference.

Intended audience

Prospective customers of NoFrixion, partners and other interested parties who wish to obtain more information on Electronic Money Institutions and NoFrixion.

It is not intended as a legal interpretation nor as part of any contractual documentation between NoFrixion and any prospective or current customer.

Table of contents

Executive Summary

Following authorisation as an Electronic Money Institution in July 2023, NoFrixion became a regulated financial institution subject to the regulatory oversight of the Central Bank of Ireland.

While an EMI is not a bank, many EMIs provide services which banks have traditionally provided – payments services in particular.

EMIs have emerged as an important part of the banking and payments ecosystem, and are especially associated with ‘challenger banks’ and ‘payment service providers’.

Well known EMIs include Revolut, Paypal, Stripe, Monzo and Wise, some of whom have gone on to become banks (or Credit Institutions as they are more properly known). In Ireland there are 26 EMIs which is an unusually large number relative to Ireland’s population. This is because most are major UK and US firms (Stripe etc). While the minimum authorisation requirements for an EMI are standard, it is important to note that almost all EMIs in Ireland are large multinationals - NoFrixion is the only indigenous tech company authorised as an EMI.

One of the main reasons for the emergence of EMIs is that traditional banks have struggled to keep pace with technological change, especially in the payments industry.

The concept of EMI came about to enable Financial Technology companies (Fintechs) to provide advanced technical solutions, better customer experience and innovative products while ensuring that customers were protected by effective regulatory oversight.

The most important aspect of an EMI’s operation, from a customer funds point of view, is that the EMI never handles funds directly – all funds are held with a credit institution. In NoFrixion’s case, the Credit Institution does not lend money either – it exists purely as a deposit taking institution and holds all funds on overnight deposit with the Central Bank of Luxembourg – a AAA-rated institution.

This document explains how an EMI operates from a regulatory and technical perspective and provides some context on why EMIs exist, and why they have become an integral and essential part of the financial services ecosystem.

Regulatory Landscape

In the EU (and UK), Fintechs become regulated institutions and obtain access to the European and global financial systems, in one of four ways (in order of difficulty):

1. AISP/PSP which provides Open Banking services.
2. Payment Institution which provides payment services
3. Electronic Money Institution which provides payments services and electronic money
4. A Credit Institution (commonly known as a bank)

AISP/PSPs provide relatively simple services. While the regulatory process is robust, the requirements are far less onerous than the next categories with minimal capital requirements.

A Payment Institution is effectively authorised to provide payments services – these are most often e-commerce payments services – providing card processing services, and prepaid money cards. Payment Institutions must maintain minimum capital up to €125,000.

An Electronic Money Institution can provide all of (1) and (2) along with electronic money. Electronic money can be thought of as the ability to hold customer funds indefinitely (a more detailed description is provided later in this document). As a result of holding customer funds, an EMI is required to maintain minimum capital of €350,000 or 2% of electronic money (customer funds) whichever is the greater.

A credit institution can pay interest and grant credit along with all of the services listed above. An application is very rare these days due to the enormous complexity and cost, and because an EMI can provide the majority of services.

The capital requirements for EMIs and Credit Institutions are calculated using Common Equity Tier 1 (CET1) which is a component of Tier 1 Capital. The implementation of CET1 started in 2014 as part of Basel III regulations relating to cushioning a local economy from a financial crisis.

NoFrixion Authorisation

Following authorisation as an Electronic Money Institution in July 2023, NoFrixion became a regulated financial institution subject to the regulatory oversight of the Central Bank of Ireland.

One of the most important aspects of an EMI is that customer funds are safeguarded with a credit institution (an EU Bank). In fact, NoFrixion are not in possession of funds directly at any point. NoFrixion issue instructions on behalf of customers to the underlying credit institution to move funds. The next section explains how this works in detail.

How NoFrixion Process Payments

Upon authorisation, NoFrixion opened a safeguarding account with Banking Circle, a credit institution authorised in Luxembourg. The safeguarding account can only be opened post-authorisation. Banking Circle do not lend money themselves – they are purely a deposit taking institution. A safeguarding account is a specific account protected by law, designed for use by electronic money institutions.

In parallel, NoFrixion applied to the Banking and Payments Federation of Ireland (BPFI) for a National Sort Code. The BPFI administer sort codes in Ireland.

They then applied for a Legal Identifier Code – an international code to identify parties in financial transactions.

Once NoFrixion received the National Sort Code and Legal Identifier Code, they applied to SWIFT for a Bank Identifier Code.

Upon receipt of the Bank Identifier Code (BIC), NoFrixion applied for membership of the SEPA schemes – SEPA Credit Transfer, SEPA Instant and SEPA Direct Debit.

An EMI cannot connect directly to SEPA and must connect via a ‘sponsor bank’ which is typically the safeguarding bank. In NoFrixion’s case, this is Banking Circle.

Once all information was supplied to Banking Circle (the safeguarding bank), Banking Circle informed their supplier (the German Central Bank – Bundesbank) that NoFrixion was their customer and that all SEPA transactions for NoFrixion’s BIC were to be sent to Banking Circle.

It is worth noting that of the 6000 or so banks in Europe, only around 250 connect directly to SEPA. None of the Irish retail banks connect directly to SEPA and use other banks in the same way that NoFrixion do. This partially explains why it is difficult for them to support SEPA Instant for example.

NoFrixion BIC, NSC and IBAN

IBAN range:	NFXN IExx 91 00 01 XX XXXX
Bank Identifier Code (BIC):	NFXNIE22
National Sort Code:	91-00-01
LEI:	63400JLPGXLBL3ZOQ96

IBANs are constructed of the BIC and Sort Code plus the account number. NoFrixion's IBANs are reachable from any institution connected to SEPA and SWIFT.

European Payments Council (EPC)

NoFrixion is a member of the SEPA schemes including SEPA CT, SEPA Instant and SEPA DD. See here on the EPC (European Payments Council):

https://www.europeanpaymentscouncil.eu/what-we-do/be-involved/register-participants

The EPC manage the SEPA schemes.

SEPA Membership

A list of all SEPA participants can be found here:

(NoFrixion is listed on page 67, 12 lines up from end)

https://www.europeanpaymentscouncil.eu/sites/default/files/participants_export/sct/sct.pdf?v=1717713123

SWIFT membership

NoFrixion are indirect participants of SWIFT, with Bank Identifier Code NFXNIE22

Payment Instructions & Fund Movement

When a payment to a NoFrixion IBAN is submitted to SEPA for payment, SEPA look up the BIC and send the instruction to the German Bundesbank, who send it to Banking Circle. Banking Circle know this payment is for a NoFrixion IBAN, and inform NoFrixion of the payment.

Banking Circle however, deposit the funds into the Safeguarding Account where they remain.

NoFrixion update the customer ledger to reflect the funds received.

When a NoFrixion customer sends a payment, NoFrixion transmit the instruction to Banking Circle, who forward the instruction to SEPA and debit the funds from the Safeguarding Account. Once confirmed as sent, NoFrixion update the customer ledger to reflect the new balance.

Safeguarding Audit

The system of safeguarding accounts and access to SEPA ensures that NoFrixion as an EMI can safely provide these services with the underlying support of a regulated credit institution.

NoFrixion is one of the only EMIs firms to implement real time reconciliation on ledger and safeguarded funds. This is further confirmed at end of day with exception alerts which are a priority one alert, informing senior management. This approach was designed from the outset to meet the strict requirements of the CBI who have made safeguarding one of their priorities.

EMIs are required to prepare a detailed document/report setting out a description of aspects of their organisational arrangements in place to secure their compliance with the relevant safeguarding requirements. They are also required to prepare an assertion document signed by the company's Board of Directors that, in all material respects, the document fairly represents the situation at the date of the report.

EMIs in Ireland are further required to have an independent Safeguarding Audit carried out, on an annual basis, by a qualified 3rd party.

The statutory auditor (or other audit firm) will perform a reasonable assurance attestation engagement, in relation to the firm's assertion as signed off by the Board of Directors.

The Central Bank in its role as the competent authority responsible for the oversight of EMIs considers Safeguarding of Funds to be of critical importance per the Board assertion and the Safeguarding Audit requirements as outlined above. More details from the Central Bank are provided here for information:

https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/payment-institutions/safeguarding-notice-to-piemis-published-25-may-2023.pdf

NoFrixion appointed Eisner Ampner as the firm's Internal Auditor, and this engagement has been registered with the Central Bank of Ireland.

Central Bank Reporting

Electronic Money Institutions in Ireland have several regulatory reporting responsibilities to the Central Bank of Ireland. These include regular and ad hoc reporting requirements designed to ensure compliance with financial regulations and maintain transparency.

Regular Reporting

1. **E-Money Institution Accounts Return**: EMIs must submit quarterly returns, detailing their financial accounts (Income Statement and Balance Sheet).
2. **E-Money Supplementary Return**: The supplementary return must also be submitted quarterly, providing additional financial details, including minimum capital requirements and details of safeguarded funds.

Audit Reporting

1. **Annual Audited Accounts**: EMIs are required to submit their annual audited financial statements within six months of the financial year-end.
2. **Statutory Duty Confirmations**: Following the annual audit, the external auditor must submit a statutory duty confirmation to the CBI. This includes confirming whether any reportable issues arose during the audit.
3. **Safeguarding Audits**: EMIs must conduct specific audits to ensure compliance with safeguarding requirements under the European Union (Payment Services) Regulations 2018 (PSR) and the European Communities (Electronic Money) Regulations 2011 (EMR). These audits must be conducted by an external auditor, and a detailed report must be submitted directly to the CBI.

External Assessment – Auditor (Eisner Ampner)

In reference to the Central Bank of Ireland's Dear CEO letter of 20 January 2023 and in particular the requirement that payment and e-money firms obtain a specific audit of their compliance with the

safeguarding requirements under the PSR/EMR by 31 July 2023, EMIs are required to obtain an external safeguarding audit.

Following discussions with Chartered Accountants Ireland (CAI), an acceptable format for these engagements has been agreed. EMIs are required to prepare a detailed document setting out a description of aspects of their organisational arrangements to secure their compliance with the relevant safeguarding requirements under the Electronic Money Regulations. EMIs should also prepare an assertion, approved by the Board of directors, stating that in all material respects that (1) the description is fairly presented, and (2) the controls and processes included in the description were operating as described at the reference date. Further details are available here:

https://www.charteredaccountants.ie/docs/default-source/technical-documents/technical-releases-alerts/tr01-2023-safeguarding-reports-for-emoneyfirms.pdf

Board of NoFrixion

nofrixion

Kieran McLoughlin, Chair

Founder & Managing Partner, VentureWave Capital

Board Member, Glucksman House NYU
Board Member, The John & Pat Hume Foundation
North American Advisory Board Member, UCD Smurfit School
Advisor to the Board, Endeavour Ireland
Formerly President & CEO, The Ireland Funds Worldwide

Kate Hotten, Independent NED, Chair of Risk & Technology Committee

Senior Advisor, FINTRAIL
Landscape Architect

Formerly STRIPE, International Head of Financial Crime & Executive Director
Formerly Wells Fargo, Anti-Bribery & Corruption Officer

Patrick Pinschmidt, Non-Executive Director

Managing Partner, Middlegame Ventures

Formerly Senior Advisor, RegTech Labs
Formerly Deputy Assistant Secretary US Treasury Department
Formerly Financial Markets Policy Advisor, Congressional Oversight Panel
Formerly VP US Equity Research, Morgan Stanley

Maurice Roche, Non-Executive Director

General Partner, Delta Partners

One of Ireland's oldest and well known VC firms.

Colm O'Sullivan, Non-Executive Director

Managing Partner, Further VC

Formerly Ventures Principal, Climate Investment
Formerly Investment Professional, Pioneer Point Partners
Formerly Investment Analyst, Triple Point Investment Management

Executive Team

nofrixion

Feargal Brady, CEO

Formerly co-founder & CEO Blueface

Appointee of Enterprise Ireland to Ireland for Finance Committee.

Aaron Clauson, CIO/CTO

Formerly co-founder & CTO Blueface

Formerly developer of SipSorcery, and open source projects currently used by US multinational telecoms providers.

Ruairi deBurca, Head of Anti-Financial Crime & MLRO, Acting CRO

MSc Forensic Computing & Cybercrime Investigation
Bachelor of Civil Law, UCD
Formerly Onsite Supervisor, Central Bank of Ireland
Formerly Lead Inspector of Supervision, Retail firms, Central Bank of Ireland

Michael Culligan, Chief Compliance Officer, Head of Strategy

C.Dir, Chartered Director, Institute of Directors
Formerly CEO, Dublin BIC
Formerly Venture Partner, Further VC
Founder, DBIC Ventures Seed Fund
Formerly Director, Guinness Enterprise Centre

Brian Quigley, Head of Finance

FCA, Chartered Accountants Ireland
M.ACC Master of Accounting, UCD
Formerly VP Finance, TrueLayer
Formerly Financial Controller, Stripe
Formerly International Accounting Manager, Facebook

nofrixion

Frequently Asked Questions

What is the difference between an EMI and a bank?

NoFrixion is not a bank, but is authorised to provide many of the services which banks have traditionally provided – however it cannot pay interest (directly) or grant credit. It is not designed to be a deposit taking institution, but rather a facilitator of payments.

In reality, a bank is a deposit taking entity which also provides payment services, while an EMI is a specialist in money movement and payment services.

An EMI will generally have very modern technology designed for today's fast-moving world.

Are my funds guaranteed / does the deposit guarantee scheme apply?

Funds deposited with a bank in the EU are guaranteed by the government to a maximum of €100,000, under the Deposit Guarantee Scheme. This guarantee does not apply to an electronic money institution - this is because an EMI must safeguard 100% of all customer funds. This is in contrast with a credit institution which uses customer deposits to provide loans. All NoFrixion funds are ringfenced and separated from NoFrixion operating funds by law.

The €100,000 is chosen as most depositors would not have such large deposits, and so the guarantee helps to ensure that a 'run' on a bank does not happen.

A bank might fail - as happened in the EU and Ireland in recent times - because banks lend money and don't always get repaid. (In fact, a deposit with a bank is actually a loan to the bank who promise to repay it).

An Electronic Money Institution cannot lend customer funds, and must maintain them in their entirety, in a specific type of segregated account, which is legally protected from creditors.

Are my funds safe?

NoFrixion is required by law to safeguard customer funds, and to hold them with an EU Credit Institution. In fact, NoFrixion do not hold funds directly at all.

In summary:

1. Customer funds are ring fenced and protected by law. In the event that NoFrixion became insolvent, these funds cannot legally be used to pay creditors and MUST be returned to account holders.
2. As part of NoFrixion's authorisation by the Central Bank of Ireland, NoFrixion must maintain a 'Wind Down Plan', which details exactly how funds are to be returned to customers in the event of a wind down.

3. This plan is monitored by the board, and is required to be implemented if there is a chance that NoFrixion may become insolvent within 6 months.
4. NoFrixion must maintain a minimum capital adequacy of €350,000 to ensure that staff and external parties can be engaged to effect the return of customer funds and an orderly wind down. Any such wind down would be overseen by the Central Bank of Ireland.
5. NoFrixion must report quarterly to the Central Bank of Ireland, on capital adequacy and solvency.
6. NoFrixion must perform daily checks to ensure the accuracy of the Safeguarding account and the customer ledger balances.
7. The policies and procedures governing Safeguarding are extensive and are approved by the Central Bank of Ireland, and audited to ensure compliance by an external auditor
8. NoFrixion is audited on an annual basis under two regimes - the standard financial audit, and the regulatory audit - both carried out by different external firms.

What is a 'Safeguarding Account'?

The method of ringfencing customer funds under the PSD2 legislation is known as 'Safeguarding'. A safeguarding account is a specific type of bank account designed for the purposes of segregating and securing customer funds and must be maintained with an EU registered bank.

Are my funds held separately from NoFrixion funds?

NoFrixion's contract with the safeguarding bank includes the specific clauses which form part of the regulatory requirement of PSD2. This includes a clause to ensure that NoFixoin cannot co-mingle NoFrixion funds with customer funds:

NoFrixion are under an obligation to keep money we hold belonging to our customers ***separate from our own money*** *pursuant to article 10 of Directive 2015/36/EU on payment services and article 7 of Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions and any local implementation thereof. We have opened the Safeguarding Accounts for the purpose of depositing money with Banking Circle belonging to our customers.*

Are my funds protected by law from creditors of the Safeguarding Bank?

NoFrixion's contract with the safeguarding bank includes the following clause which form part of the regulatory requirement of PSD2:

Banking Circle ***does not have any interest in, or recourse or right against, money held in the Safeguarding Accounts*** *for any sum owed to Banking Circle, or owed to any third party, except as permitted by applicable law. This means, for example, that Banking Circle shall not have any right to combine the Safeguarding Accounts with any other account and shall not have any rights of lien or*

pledge, set-off, retention or counterclaim, security interest against money held in the Safeguarding Accounts.

In case of insolvency, bankruptcy or in any other situation of equal ranking, the funds are not part of the mass of our assets and can neither be used as a guarantee by us to cover our obligations or those of third parties, nor be seized whether by our creditors or creditors of our customers.

What happens if NoFrixion is wound-up?

NoFrixion's contract with the safeguarding bank includes the following clause which form part of the regulatory requirement of PSD2:

Banking Circle shall be ***required to release on demand*** ***all money standing to the credit of the Safeguarding Accounts on proper notice and instruction from NoFrixion or a liquidator,*** *receiver, administrator, or trustee (or similar person) appointed for NoFrixion in bankruptcy/insolvency (or similar procedure),* ***in any relevant jurisdiction****.*

Creditor request to release safeguarded funds?

In the event that a creditor of NoFrixion, or of Banking Circle, attempts to claim those funds held in the account, *Banking Circle* are contractually obliged to respond as follows:

In the case of seizure of the money held on the Safeguarding Accounts or the exercising of other rights in relation to the money held on the Safeguarding Accounts by a third party or any attempted action of a foregoing nature Banking Circle will inform the seizing creditor or the relevant third party of the Safeguarding Account's status as a safeguarding Account.

Who is NoFrixion's Safeguarding Bank?

NoFrixion use Banking Circle as its safeguarding bank.

NoFrixion chose a 'deposit-only' bank as its Safeguarding account provider. The bank is authorised, and has its headquarters, in Luxembourg. It also maintains a branch in the United Kingdom.

What credit rating is NoFrixion's safeguarding bank?

NoFrixion's safeguarding bank does not lend against deposits (which means that it does not have a credit rating).

However, all funds are maintained overnight in cash deposits in the **Central Bank of Luxembourg. The Central Bank of Luxembourg is AAA rated.**

According to Fitch: AAA' ratings denote the lowest expectation of default risk. They are assigned only in cases of exceptionally strong capacity for payment of financial commitments. This capacity is highly unlikely to be adversely affected by foreseeable events.

It should be noted that no Irish banks (of which NoFrixion are aware) provide safeguarding accounts, and very few in Europe.

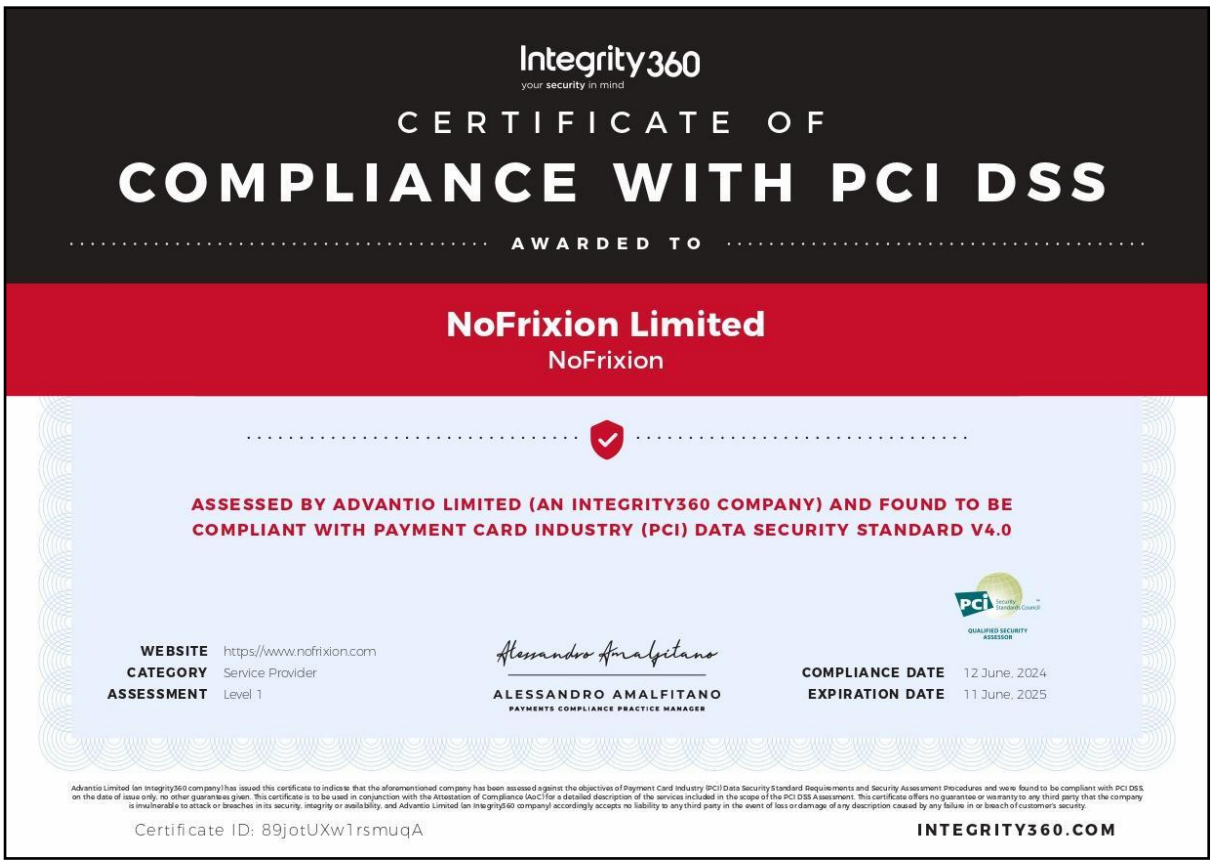
Link to CBI Register showing NoFrixion's Authorisation

NoFrixion is authorised by the Central Bank of Ireland as an EMI (Electronic Money Institution), licence number: C458163. See register here:

https://registers.centralbank.ie/FirmDataPage.aspx?firmReferenceNumber=C458163

Is NoFrixion PCI compliant?

NoFrixion is compliant with the latest version of PCI DSS (Payment Card Industry Data Security Standard), version 4. This is an annual audit and the latest was completed in June 2024. NoFrixion is compliant to the highest level 1 of the standard. The audit includes a four day penetration testing of the NoFrixion IT systems. A copy of the Cert is shown below.



How did NoFrixion obtain an authorisation as an EMI?

The basic EMI application consists of a minimum of the following information:

1. Completed Application Form
2. Programme of operations setting out the exact payments services to be provided.
3. Detailed business plan including three year financial projections
4. Evidence of initial capital
5. Detailed description of safeguarding policy and measures to safeguard customers funds
6. Description of governance and internal control mechanisms to demonstrate they are proportionate, appropriate, sound and adequate.
7. Description of security policies including monitoring and incident management and reporting plan
8. Description of the processes to file, monitor, track and restrict access to sensitive payment data
9. Description of business continuity arrangements including reaction to IT, security and other external events impacting customer operations
10. Description of procedure for the collection of statistics on performance, transactions and fraud
11. Security policy document including business wide risk assessment
12. Description of internal control mechanism to comply with anti-money laundering and terrorist financing obligations
13. Description of structural organisation including roles and responsibilities, reporting lines and implementation of risk mitigation using three lines of defence model
14. A wind-down plan describing the procedure for returning customer funds in the event of a liquidation.
15. The identity of the promoters and their suitability and relative experience
16. The identity of the directors and management and evidence of their fitness and probity for their respective role and responsibility.
17. The identity of the statutory auditors.
18. The identity of the internal auditor
19. The identity and evidence of suitability for the role of:
    a. Chair
    b. Non-executive director(s)
    c. CEO
    d. COO/CIO
    e. CTO
    f. Head of Finance
    g. Anti-Money Laundering and Reporting Officer / Head of Anti-Financial Crime
    h. Chief Risk Officer
    i. Chief Compliance Officer
20. Legal status and corporate structure

NoFrixion Policies & Procedures

In addition to the basic information above, an extensive set of policies and procedures which document every aspect of the operation of the business is required to be submitted for analysis and approval. NoFrixion's document library contains 145 documents which govern the operation of the company and ensure compliance with regulatory and statutory requirements.

Whilst some documents are confidential (especially regarding security and anti-fraud and money laundering), a sample list of documents is shown below:

Risk & Operations

1. Technology and Risk Committee Terms of Reference
2. Risk Management Policy
3. Risk Management Framework

Safeguarding & Outsourcing

4. Safeguarding Policy
5. Outsourcing Policy
6. Outsourcing Risk Assessment & Due Diligence Form
7. Outsourcing Remote Customer Onboarding Solution Assessment Form
8. Outsourcing Register

Internal Audit & Assurance

9. NoFrixion Internal Audit Charter
10. NoFrixion Internal Audit Strategy 2023-2025
11. Fitness & Probity Assurance Testing & Monitoring Procedure
12. Outsourcing Assurance Testing & Monitoring Procedure
13. Data Protection Assurance Testing & Monitoring Procedure

Business Continuity & Incident Management

14. Business Continuity Policy
15. Business Continuity Context, Requirements and Scope
16. Business Continuity Management Plan
17. Business Continuity Plan
18. Business Impact Analysis
19. Incident Management Policy & Procedure

WInd-down and Migration

20. Wind Down Procedure
21. Wind Down Plan Addendum
22. High Level Migration Plan

Information Security

23. Information Security Management System Scope Document
24. Information Security Policy
25. Security Awareness and Acceptable Usage Policy
26. Password Policy

27. Change Management Policy
28. Secure Development Policy
29. Paper and Electronic Media Policies
30. Network Security Administration Policy
31. Policy Additions for PCI DSS
32. Security Configuration Policy
33. Anti-Virus Policy
34. Backup Policy
35. Encryption Policy
36. Special Technologies Policy
37. Software Development Policy and Procedures
38. Employee Identification Policy
39. Logging Controls Policy
40. Cloud Security Policy

Data protection & Access Control

41. Data Protection Policy
42. Data Processing Register
43. Data Protection Impact Assessment Template
44. Data Classification Policy
45. Information Security Access Control Policy
46. Information Security Privileged Access Groups Register
47. Information Security Privileged Access Monitoring Procedure
48. Incident Response Plan
49. Payment Data Handling Procedure
50. IT Staff Responsibilities Policy

Governance & Operations

51. Board Terms of Reference
52. Functional Overview
53. Data Processing Agreement
54. Statement of Technical and Organisational Measures

Terms & Conditions

55. Framework Contract/ General Terms & Conditions
56. Services Agreement
57. NF EU Terms & Conditions
58. NF UK Terms & Conditions
59. Website Terms of Use
60. Privacy Policy
61. Non-Disclosure Agreement/ Confidentiality Agreement

People & Culture

62. Health & Safety Policy
63. Staff Onboarding Policy
64. Basic Fitness & Probity Questionnaire and Confirmations
65. PCF/CF Fitness & Probity Questionnaire and Confirmations
66. Employee Privacy Notice

67. Staff Handbook
68. Code of Ethics
69. Equality, Diversity & Inclusion Policy
70. Staff Exit Checklist
71. Conflict of Interest Policy
72. Code of Conduct
73. Breastfeeding Policy
74. NoFrixion Social and Environmental Statement
75. Grievance & Disciplinary Procedure
76. Grievance & Disciplinary Log
77. Policy Management Framework Policy

What is NoFrixion's ESG policy

NoFrixion became a B Corporation in 2023, the first Irish Financial Institution to become a B Corp and the only regulated firm of its kind to date.

B Corp Certification is a designation that a business is meeting high standards of verified performance, accountability, and transparency on factors from employee benefits and charitable giving to supply chain practices and input materials. In order to achieve certification, a company must:

- Demonstrate **high social and environmental performance** by achieving a B Impact Assessment score of 80 or above and passing independent risk review.
- Make a **legal commitment** by changing their corporate governance structure to be accountable to all stakeholders, not just shareholders, and achieve benefit corporation status if available in their jurisdiction.

- Exhibit **transparency** by allowing information about their performance measured against B Lab's standards to be publicly available on their B Corp profile on B Lab's website.

Further Information, regulatory references, glossary

Electronic Money Institutions

An e-money institution (EMI) is an undertaking that has been authorised to issue e-money in accordance with the European Communities (Electronic Money) Regulations 2011, as amended (EMR).

E-Money

According to the Central Bank of Ireland, e-money can therefore be defined as monetary value as represented by a claim on the issuer, which is:

- electronically stored
- issued on receipt of funds for the purposes of making payment transactions
- accepted as means of payment by a natural or legal person other than the issuer

Reference:

https://www.centralbank.ie/regulation/industry-market-sectors/electronic-money-institutions

Payment Services Directive II (PSD2)

The specific legislation in Ireland, transposing the European Payment Services Directive (PSD2) is available here: https://www.irishstatutebook.ie/eli/2018/si/6/made/en/print

European Policy Context

The EU has been promoting greater competition in Financial marketplaces. It is doing this under an EU Directive known as PSD2 that applies to payment services in the EU. PSD2 has been law in Ireland since 2018.

PSD2 aims to provide for the further development of a better-integrated internal market for electronic payments within the EU. It puts in place a comprehensive framework for payment services, with the goal of making payments within the EU more efficient and secure. It also seeks to open up payment markets to new entrants, with a view to encouraging more competition.

The EBA (European Banking Authority), an agency of the EU, is an independent EU Authority. It is tasked with implementing a standard set of rules to regulate and supervise banking across all EU countries. Its aim is to create an efficient, transparent and stable single market in EU banking products. It plays a key role in safeguarding the integrity and robustness of the EU banking sector.

The EBA develops requirements to bring about a level playing field in the EU for the authorization and supervision of payment services providers. The EBA also promotes competition and facilitates innovation in payments.

Per the EBA the revised Payment Services Directive (PSD2) has been applicable since 13 January 2018 and sets out the requirements that applicants must meet in order to be authorised as payment institutions (PIs) and electronic money institutions (EMIs).

Compliance and adherence to PSD2 is overseen in Ireland by the Central Bank of Ireland

EMIs are governed originally under European Parliament Directive 2009/110/EC transposed into Irish law in 2009 and further updated when the EU Payment Services Regulation (PSR) came into effect in 2018. This transposed into Irish law the EU Directive 2015/2366 on PSD2 (Payment Services Directive 2).

Irish EU Commissioner for Financial services, Financial stability and Capital Markets Union, Mairead McGuinness has responsibility for this arena for the EU.

Cyber Security & Resilience Overview

Infrastructure & Security

Architecture

Our architecture is multi-tenant by design and robust controls are applied to ensure that access to data is restricted based on a user's job role and associated access privileges.

Industry standard protocols, such as OAuth2, are used to facilitate secure access to third-party integrations. Since inception, NoFrixion has developed its Information Security System in alignment with ISO 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems.*

Encryption

Data in transit is encrypted using SSL certificates (TLS 1.2) meaning that unauthorised individuals cannot decipher confidential financial information.

Hosting Provider

NoFrixion uses Azure and AWS for data hosting services. AWS is ISO 27001 certified and maintains SOC 1 and SOC 2 reports.

Controls

Our approach streamlines international payments within a regulated proprietary network, with best-in-class compliance controls embedded within the payment process.

Data Security

Data retention and deletion

We only retain data for as long as is required under regulatory and legislative requirements. Data retention timelines are defined, and procedures are in place to comply with erasure requests from our clients.

Security of Data Processing activities

NoFrixion is headquartered and registered in Ireland and subject to the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679). Technical and organisational controls are implemented and maintained as per industry best practice

Awareness & training

Staff undergo mandatory annual training, developers and ICT staff also complete technical training that includes material from relevant globally recognised risks

Security Testing

Patch Management

A risk-based approach is taken with all critical patches installed within 7 days or less in line with our patch management standard

External Audits

A dedicated audit program is in place with several internal audits completed on a quarterly basis and annual external audits by our PCI-DSS certifying body, Integrity 360. Ongoing penetration testing is conducted on cloud services.

Penetration Testing

Testing is conducted annually by our third-party provider. Vulnerabilities are assigned owners and tracked to remediation in our IT governance and management forums.

Security Incident and Event Notification

24/7 system monitoring, has a documented and established incident management procedure with incident severity and points of escalation defined.

Resilience

Backup

NoFrixion implements backup and disaster recovery processes to ensure data integrity and service continuity. Point in time incremental and regular full backups are conducted, and data replication techniques are employed to minimise data loss in the event of a failure.

Disaster Recovery

A comprehensive, tested, ICT Disaster Recovery Plan (DRP) is in place to facilitate swift recovery in case of system failures or disasters.

Cloud

NoFrixion uses a cloud deployment model, utilising EU-based data centres and dual cloud providers (AWS & Azure) subject to stringent digital operational resilience and data protection legislation. Our core platform uptime target is 4 nines availability. In addition to contractual requirements, third-party suppliers are also subject to international standards.