fintech **OS**

Lexis Nexis Connector 1.0

User Guide

TOC

Overview

Connectors are simple, data point connections to external Saas providers, that are used to enrich internal customer data to help in onboarding and risk decision scenarios. API Connectors gather data from a collection of REST APIs with the purpose of merging them into a cloud-based data storage system. This process gives the possibility of filtering and transforming data into a proper format or structure for the purposes of querying and analysis.

FintechOS offers the possibility of accessing different databases with the purpose of moving around specific data using API connectors. They can be used but are not limited to banking or insurance business scenarios, such as customer identity verification in a loan origination operation, automatically fill-in customer data, and so on. In addition, connectors can have a significant role in a business's risk management process by providing easy access to databases where information regarding financial risks is stored.

LexisNexis Bridger Insight XG is a platform that accesses identity verification, screening, due diligence and fraud prevention services in order to efficiently aid the Know Your Customer (KYC) processes and to make sure the institution is compliant with financial regulations.
The FintechOS Lexis Nexis Connector simplifies the customer verification process by allowing financial institutions to easily add it to their digital journey. Once integrated to the digital journey, the API connector calls a number of REST APIs in order to retrieve the following data:

- Basic person search to retrieve information such as name, date of birth, address, gender, and so on.

- Basic company search to retrieve information such as name, address, registration number, and so on.

- Full search to retrieve any possible information either person or company data.

In addition to aiding and accelerating account openings, the LexisNexis Bridger Insight XG simplifies SWIFT, International ACH and FedWire Payment Screening. It helps fight financial crime by supporting the resolution of critical BSA/Anti-Money Laundering (AML) and Customer Identification Program (CIP) and KYC compliance requirements. As a result, it reduces risk exposure with enhanced due diligence data.

When accessed from a digital journey, the Lexis Nexis Connector allows bank clerks to collect and verify data from multiple systems. It can be further enhanced via FintechOS Studio adapting it to business requirements. The result is a fully functional and personalized searching tool that collects the needed information in a few steps.

Business Pain Points

The Lexis Nexis Connector is aimed at resolving some of the pain points when searching fraud databases for individual or business data:

- searching in fraud databases is time consuming and the data retrieved lacks important details

- it can be challenging to spot false positives

- the needed information can be scattered throughout databases

- requires verified and updated information

- limited time to analyze the data found

- the Know Your Customer (KYC) process can be complex when accessing fraud databases for identity verification or screening

Key features

Once integrated in a digital journey, the Lexis Nexis Connector solves these pain points by offering a simple way to collect data from multiple fraud databases.

- The data returned from the search is detailed.

- The complex search mechanism helps reduce false positives.

- Single point of entry for a consistent search.

- Easy to use. It can be added to a digital journey to simply the search process.

- Time-efficient. The data no longer needs to be added manually.

- The retrieved information is verified.

- Speeds up the Know Your Customer (KYC) for better efficiency by accessing multiple fraud or potential fraud databases through one access point.

Installation

Follow the bellow steps to install FintechOS Lexis Nexis Connector.

Prerequisites:

1. Download the package from FintechOS Marketplace.

2. Obtain the Lexis Nexis user role, name, and password.

   > **NOTE**
   >
   > The user role, name, and password are obtained by the customer from
   >
   > Lexis Nexis once a contract is established.

3. Install the package on an environment FintechOS 21.1.6.0 and above with the Innovation Studio, Portal and B2C Portal configured. For details on B2C, see Setting B2C Environment.

4. Configure the **JobServer**. For information regarding FTOS JobServers, see the JobServer section from the Core DPA Platform 2 Administration Guide.

Import Packages:

1. Open the FintechOS Innovation Studio, navigate to the **DevOps** menu, select the **Deployment Packages**. The Deployment **Packages List** page opens.

2. At the top-right corner of the page, click the **Import deployment package** icon. The Open pop-up appears.

> **NOTE**
>
> For details on how to import, see Importing a Deployment Package.

Browse for the deployment package and import **LexisNexisConnector-1.0.xml**.

The script starts running in your Windows console. Wait for it to finish. If the parameter values were correct, the Lexis Nexis Connector installation is successful.

Set up web.config keys:

In the physical location of the installed digital journey, fill in the values of the key's bellow with the values available for the client:

- `<add key="lexn-role-type-role" value="" />`

- `<add key="lexn-url" value="" />`

- `<add key="lexn-client-id" value="" />`

- `<add key="lexn-password" value="" />`

- `<add key="lexn-user-id" value="" />`

The web.config setup should have the following form:

```
<add key="lexn-role-type-user" value="UserName" />
<add key="lexn-role-type-role" value="UserRole" />
<add key="lexn-url" value=
"https://staging.bridger.lexisnexis.eu/LN.WebServices/11.0/XGServic
es.svc/Search" />
<add key="lexn-client-id" value="ClientID" />
<add key="lexn-password" value="UserPassword" />
<add key="lexn-user-id" value="UserID" />
```

> **IMPORTANT!**
> The `<add key="lexn-url" value="" />` URL displayed in the above snipped is

for example purposes only. All keys are obtained by the customer from Lexis Nexis once a contract is established.

Solution Walkthrough

The FintechOS Lexis Nexis Connector offers the possibility of accessing and retrieving individual or business information by searching in databases for fraud or potential fraud. LexisNexis Bridger Insight XG is a risk management product that aids financial institutions by simplifying and accelerating the Know Your Customer (KYC) process. In addition, when searching the Lexis Nexis databases through the connector, it allows for configurations such as: determining which settings to use, as well as storing the results in the LexisNexis Bridger Insight XG database.
LexisNexis Bridger Insight XG is the screening tool to use for individuals or business customers and their legal representatives. In addition, the Lexis Nexis platform offers access to a payment screening tool that returns alerts set within the World Compliance part of Bridger Insight XG. These features help the onboarding process of a new customer or business but it's also used for further monitoring purposes and payment screenings. This means that the financial institution is alerted if any changes that break regulatory obligations appears. The procedure is simple, a search is made by the bank clerk or anyone authorized to use the platform and results are retrieved. The returned data can either point out that no matches are found or that an alert is found. The generated alerts have a confidence score rating up to 100.

FintechOS offers the possibility of accessing Lexis Nexis databases through the Lexis Nexis Connector. In order to have access to fraud records, the below digital journey is proposed.

> **IMPORTANT!**
> The below UML walkthrough is not a representation of a stand-alone application or on how to use the FintechOSLexis Nexis Connector in a digital journey to search individual or business records in fraud databases. It represents a proposition on how to use this connecter once it is integrated in a digital journey.

Lexis Nexis Connector
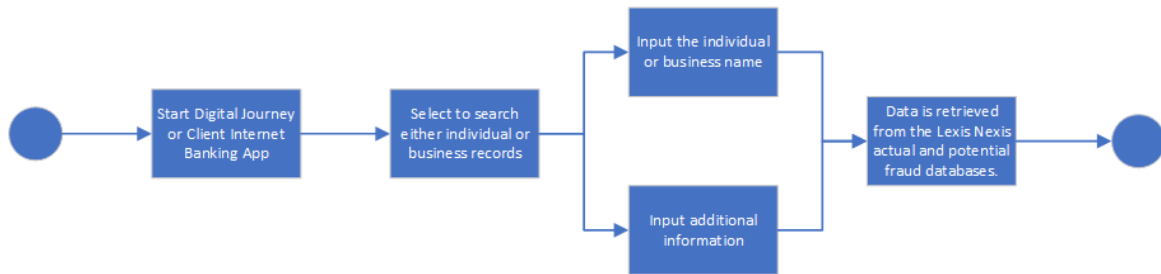
For a detailed walkthrough on how to search for company information, see the Search Lexis Nexis page. To download the diagram in Visio, click here.

Search Lexis Nexis

The FintechOS Lexis Nexis Connector offers the possibility of searching databases for any fraudulent records. Institutions can add the connector to a digital journey and retrieve records indicating fraud or potential fraud. This functionality helps lowering compliance or regulatory risk.

> **IMPORTANT!**
> The below walkthrough is a proposition on how to use the FintechOSLexis Nexis Connector in a digital journey to search individual or business records in fraud databases.

Follow the below steps to access and retrieve information using this connector.

1 Access Lexis Nexis Connector

1. Log into the FintechOS Portal using the given credentials.

2. Log into the Lexis Nexis database with the credentials provided by them

> **NOTE**
> The user role, name, and password are obtained from Lexis Nexis once a contract is established. Additional information can be found on the Installation page.

3. From the FintechOS Portal main menu expand **My Projects** and click **Lexis Nexis Connector**.

4. Select **Search Lexis Nexis**. The **Search Lexis Nexis List** page opens.

5. At the top-right corner of the screen, click the **Insert** button. The **Edit Search Lexis Nexis - Search** page opens. Fill in the following fields:

EDIT SEARCH LEXIS NEXIS - SEARCH

Select what type of search you want(ex: Individual, Business)

⦿ Individual ◯ Business

Input Data

Name

| Jane | | Doe |

| Female ▾ |

Addresses

| Baker Street | | 221B |

| United Kingdom | | London |

| NW1 6XE |

Additional Info

| Day... | | Month... |

| Year... | | Unparsed... |

| Type... | | Label... |

Config Data

| Predifined Name | Predifined Search Na... | Assign To Type | [none] ▾ ✎ | Write to database ☐ |

Context Data

| Reference | Client Reference... | DPPA | NA ▾ ✎ | GLBA | NA ▾ ✎ |

[Show results]

HINT

Only the person's first and last name and the full name of the business are mandatory to make a search. However, inputting any other information in the below fields minimizes the return of false positives records.

Field	Required	Type	Description
Individual	No	Bool	If true, the search retrieves records regarding individuals.

Field	Required	Type	Description
Business	No	Bool	If true, the search retrieves records regarding businesses.
First name	Yes	Text	The individual's first name.
Last name	Yes	Text	The individual's last name.
Full name	Yes	Text	The company's name. **NOTE** This field is visible only when the **Business** toggle button is selected.
Gender	No	Option set	The individual's gender. The following options are available: • Male • Female • Unknown • None
Address street line 1	No	Text	The first line of the address. For example, the street name.
Address line 2	No	Text	The second line of the address. For example, the street number.
Country	No	Text	The country.
City	No	Text	The city.
Postal code	No	Text	The postal code.
Day	No	Numeric	The day of the date of birth.
Month	No	Numeric	The month of the date of birth.
Year	No	Numeric	The year of the date of birth.
Unparsed	No	Text	This field contains the unstructured date value.

Field	Required	Type	Description
Type	No	Text	The information type. The following additional information type values can be retrieved: • None not - valid in a request • Citizenship • Complexion • DistinguishingMarks • DOB • EyeColor • HairColor • Height • Incident • IPAddress • MothersName • Nationality • Occupation • Other • PlaceOfBirth • Position • Race • VesselCallSign • VesselFlag • VesselGRT

Field	Required	Type	Description
			• VesselOwner • VesselTonnage • VesselType • Weight
Label	No	Text	The user-defined label. **NOTE** This label is visible when the **Type** field value is set to **Other**.
Predefined name	No	Text	This field contains a predefined search created in the LexisNexis Bridger Insight XG user interface in order to provide a more consistent search. Predefined search requires certain role access rights.
Assign to type	No	Option set	This filed contains the assignment type. The below options are available: • None • Role • User The **None** option type is not valid in a request.
Write to Lexis Nexis Database	No	Bool	If true, the information is saved in the LexisNexis Bridger Insight XG database. The default value is false.

Field	Required	Type	Description
Reference	No	Text	This field contains optional user-defined information to identify the request. For search requests, the results from this field is returned in the **Search Result** class.

Field	Required	Type	Description
DPPA	No	Option set	This field contains the DPPA (Driver's Privacy Protection Act) permissible use. The below options are available. For more details, see the Permissible Uses page. • NA • Choice0 - No Permissible Use • Choice1 - Government Agency or On Government Behalf • Choice2 - Motor Vehicle or Driver Safety • Choice3 - Debt Recovery/ Fraud • Choice4 - Litigation • Choice6 - Insurer **NOTE** The default value is **NA**. This value is not valid if a DPPA permissible use is required. This property is required for the Fraud Point Score searches or Instant ID searches on individual entities.

Field	Required	Type	Description
GLBA	No	Option set	This field contains the GLBA (Gramm-Leach-Bliley Act) permissible use. The below options are available. For more details, see the Permissible Uses page. • NA • 0 a. No Permissible Use b. Resolving Customer Disputes or Inquiries c. As allowed by the Right to Financial Privacy Act of 1978 • 1 - Transactions Authorized by Consumer • 3 - Persons with a Legal/ Beneficial Interest in the Consumer • 5 - Fraud Prevention and Detection • 6 - Required Institutional Risk Control • 7 - Legal Compliance • 12 - Persons Acting in a Fiduciary Capacity for the Consumer

Field	Required	Type	Description
			NOTE The default value is **NA.** This value is not valid if a GLBA permissible use is required. This property is required for the Fraud Point Score searches or Instant ID searches.

2 Individual or Business Data Returned

6. Click the **Show results** button. The **Edit Search Lexis Nexis - Search Result** page opens. Te following information is displayed:

Field	Required	Type	Description
Entity unique ID	No	Text	An unique system-generated number that identifies the entity.

Field	Required	Type	Description
Entity score	No	Numeric	This field displays a confidence score between **0** and **100** that LexisNexis Bridger Insight XG generates to indicate how closely the list record matched the input entity information. **NOTE** A score of **90** indicates the match is closer than a potential match with a score of **80**. When a valid score is not available, **-1** is returned.
Entity name	No	Text	The main entity name from the list record that generated the potential match.
Best name score	No	Text	The score of the name that most closely matched the input information.
Best name	No	Text	The name that most closely matched the input information.

Field	Required	Type	Description
Best country	No	Text	The country that most closely matched the input information.
Reason listed	No	Text	The reason the country is on the list.

7. Click the **Finish** button. The **Search Lexis Nexis List** page is displayed.

Permissible Uses

Permissible uses is the act of having permission to view personal information. This is a federal law requirement in conjunction with a the user agreement with the Lexis Nexis platform. The laws that apply permissible uses are the Drivers' Privacy Protection Act (DPPA) and related state laws, and the Gramm-Leach-Bliley Act (GLBA).

> **NOTE**
> If the user does not have a permissible use, then the access to personal information is restricted. Lexis Nexis databases containing non-public information that is data that can distinguish or trace an individual's identity, are made available for lawful and appropriate uses only.

The Drivers' Privacy Protection Act (DPPA) and the Gramm-Leach-Bliley Act (GLBA) permissible uses are detailed below.

DPPA Permissible Uses

The Drivers' Privacy Protection Act (DPPA) is a federal law meant to regulate the release and sharing of personal information, such as name, address, driver license number, and others, assembled by Departments of Motor Vehicles (DMVs), that became effective September 13, 1997.

> **HINT**
> When selecting a DPPA permissible use, the search is made against the drivers' licenses, motor vehicle registrations, and boat registrations for the states that recognize the permissible use selected. If **No Permissible Use** is selected. the search is not performed.

Web Service Value	Name	Description
Choice0	No Permissible Use	Used when the person does not have a DPPA permissible use.
Choice1	Government Agency or On Government Behalf	Used by government, court, or law enforcement agencies and also private person or entities acting on behalf of a Federal, State, or local agency.
Choice2	Debt Recovery/ Fraud	Used in the following scenarios: • motor vehicle or driver safety and theft • motor vehicle emissions • motor vehicle product alterations, recalls, or advisories • performance monitoring of motor vehicles, motor vehicle parts and dealers • motor vehicle market research activities, including survey research • removal of non-owner records from the original owner records of motor vehicle manufacturers

Web Service Value	Name	Description
Choice3	Motor Vehicle or Driver Safety	Used by a legitimate business or its agents, employees, or contractors only in the following scenarios: • to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; • to obtain the correct information, if the information submitted is not correct or no longer correct
Choice4	Litigation	Used in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court, or agency.
Choice6	Insurer	Used by insurer or insurance support organizations or by a self-insured entity.

GLBA Permissible Uses

The Gramm-Leach-Bliley Act (GLBA) is a federal law meant to regulate the distribution and use of materials held by financial institutions containing consumers' personal financial information, that became effective November 12, 1999.

HINT
When selecting a GLBA permissible use, the search is made against data which is regulated by the GLBA, that is contained within the Lexis Nexis database. If **No Permissible Use** is selected, the search runs is made against data not regulated by GLBA.

Web Service Value	Name	Description
0	No Permissible Use	Used when the person does not have a GLBA permissible use.
	Resolving Customer Disputes or Inquiries	Used when resolving customer disputes or inquiries.
	As allowed by the Right to Financial Privacy Act of 1978	Permitted or required in accordance with the Right to Financial Privacy Act of 1978.
1	Transactions Authorized by Consumer	Used to effect, administer, or enforce a transaction requested or authorized by the consumer.
3	Persons with a Legal/ Beneficial Interest in the Consumer	Used by someone that holds a legal interest in regards to the customer.
5	Fraud Prevention and Detection	Used to protect and prevent fraud or potential fraud, unauthorized transactions, claims, and others.
6	Required Institutional Risk Control	Used in institutional risk control programs.
7	Legal Compliance	Used in compliance with federal, state, or local laws, rules, and other applicable legal requirements.
12	Persons Acting in a Fiduciary Capacity for the Consumer	Used by a trusted person (legal representative) acting on behalf of the consumer.

Configurations Walkthrough

The following chapter of this guide is meant to explain how to use the Lexis Nexis Connector in digital journeys, as well as the technical details of how the connector helps return data.

The Lexis Nexis Connector is configurable to fit the business needs of any financial institution to help simply the verification process and reduce risk exposure. This connector can be integrated in their digital journey to have easy access to fraud databases. The information retrieved is updated and it offers a better insight on current or potential customers and businesses.

For example, in a loan origination process, where a potential customer wants to borrow a certain amount from a financial institution, along with other eligibility steps, an identity verification step is mandatory. To accelerate the screening process and eliminate any risks that the institution takes, the FintechOSLexis Nexis Connector can be accessed from their digital journey. The bank clerk searches the database for potential fraud triggering the external call to the endpoint exposed by the Lexis Nexis Connector. Then, the connector calls the LexisNexis Bridger SOAP service and the data received is saved in the connector's data model, that can be viewed in the Data Model page. Thus, the retrieved information saved in the data model is displayed in the bank clerk's digital journey allowing them to simply continue the loan origination process.

The LexisNexis Bridger Insight XG SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) APIs allows the incorporation of its functionality into existing systems such as digital journeys, banking applications, and so on. This functionality permits bank employees to manage access, search, and obtain results and lists. Each request has a SOAP message with a defined action method to perform. The REST API provides several interfaces as well (search or predefined search). Each request sends a `json` message with a defined action to perform.

For more information on how to use the connector in digital journeys and the server automation script, see the following pages:

- Using the Lexis Nexis Connector in Digital Journeys

- Server Automation Script

The image below is an UML diagram showing the Lexis Nexis search workflow. To download the diagram in Visio, click here.
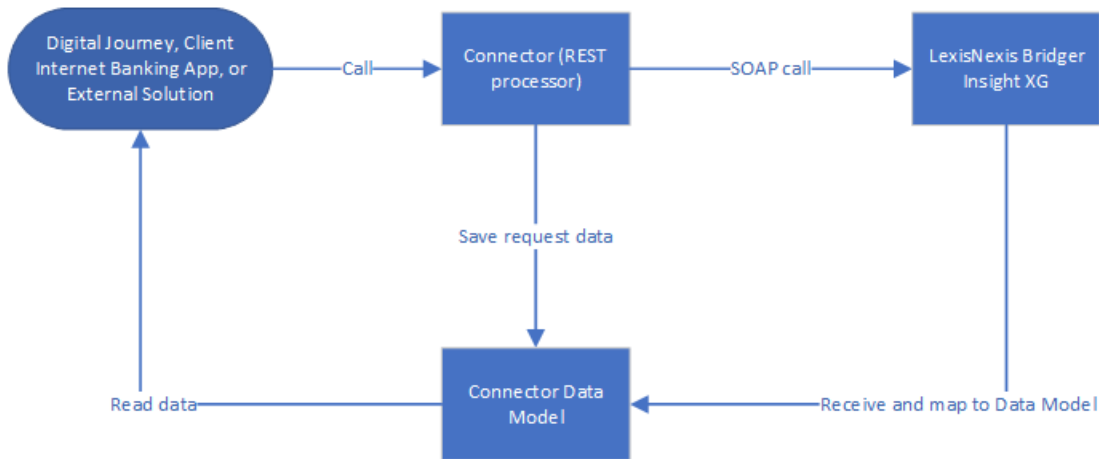
The image below is a sequence UML diagram showing the main actions that the bank clerk takes when searching for particular records. To download the diagram in Visio, click here.
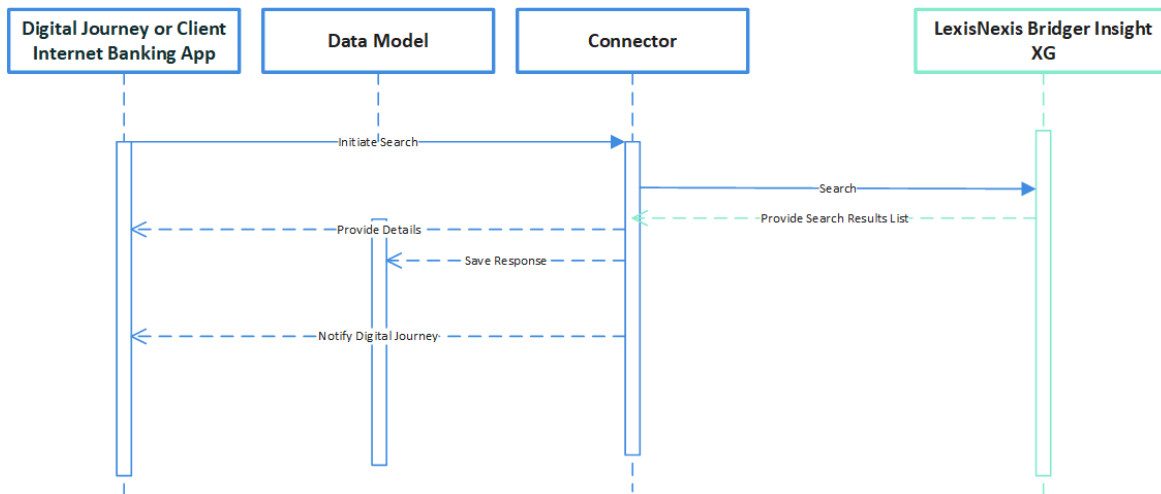
Using Lexis Nexis Connector in Digital Journeys

The Lexis Nexis Connector consists of a digital journey, a client side script, and an endpoint. Below are the steps used when calling the connector.

1. Before calling the connector, the parameters must be set. The environment settings required for the API search are set through the below variables. The Lexis Nexis platform uses a SOAP/ xml format, but the search function and the returned data is in REST/ JSON format.

Setting the Paramenters Example

```
const clientId = getAppSetting("lexn-client-id")

const password = getAppSetting("lexn-password")

const userId = getAppSetting("lexn-user-id")

const searchUrl = getAppSetting("lexn-url")

const roleTypeUser = getAppSetting("lexn-role-type-user")

const roleTypeRole = getAppSetting("lexn-role-type-role")


const searchLibraryName = "FTOS_EXTD_LEXN_Search"

const searchBindingName = "BasicHttpBinding_ISearch";

const searchWebApiClient = importWebApiClient("FTOS_EXTD_
LEXN_Search", searchUrl, "BasicHttpBinding_ISearch");


const response = searchWebApiClient.search(contextSettings,
configSettings, inputConfig)
```

2. Use the `ebs.callActionByNameAsync` function with the `FTOS_EXTD_LEXN_Search` parameter when searching for certain information from the Lexis Nexis database in the digital journey.

3. The `FTOS_EXTD_LEXN_Search` endpoint is called. The response is partially parsed at data model level and returned fully in a JSON object.

Calling from the Digital Journey Frontend Example

```
let reqObj = {

entityType: formScope.entityType,

clientReferance: formData.model.clientReference,

dppa: formData.model.dppa,

glba: formData.model.glba,

predifinedSearchName: formData.model.predifinedSearchName,

writeResultToDatabase: formData.model.writeResultToDatabase,

assingResultToEmailNotification:
formData.model.assingResultToEmailNotification,

assingResultToRolesOrUsers:
formData.model.assingResultToRolesOrUsers,

assingResultToType: formData.model.assingResultToType,

nameFull: formData.model.nameFull,

nameFirst: formData.model.nameFirst,

nameLast: formData.model.nameLast,

nameGeneration: formData.model.nameGeneration,

nameMaidenName: formData.model.nameMaidenName,

addressStreet1: formData.model.addressStreet1,
```

```
addressStreet2: formData.model.addressStreet2,

addressCity: formData.model.addressCity,

addressPostalCode: formData.model.addressPostalCode,

addressCountry: formData.model.addressCountry,

additionalInfoDay: formData.model.additionalInfoDay,

additionalInfoMonth: formData.model.additionalInfoMonth,

additionalInfoYear: formData.model.additionalInfoYear,

additionalInfoUnparsed:
formData.model.additionalInfoUnparsed,

additionalInfoLabel: formData.model.additionalInfoLabel,

additionalInfoType: formData.model.additionalInfoType,

gender: formData.model.gender,

recordId: formData.id

}

ebs.showLoadingPanel()

ebs.callActionByNameAsync("FTOS_EXTD_LEXN_Search", reqObj)

.then((result) => {

if (result.IsSuccess == true) {

ebs.showMessage("Success", "success")

formData.refreshForm()

} else {

ebs.showMessage("error", "error")

}
```

```
})
```

HINT
As a developer, the data can be obtained from the data model or from the JSON object.