Fraud Lockdown

Application Name: PS_FraudLockDownPackage.dnaxp
Application Description: Fraud Lockdown
Application: 15904

DNAapp ID 67a55242-e39a-45a3-a95c-c7cfba534b70

Overview:
This application enables users to initiate a person level Fraud Lockdown process which locks down the accounts and persons whenever a fraud is identified.

Key Benefits:
This solution increase user efficiency by automating a number of tasks that would otherwise be manual.

Processing:
The fraud lockdown process includes following activities:

- Add lockout and/or warning flags to the selected person record.
- Add lockout and/or warning flags and notes to accounts where the selected person holds institution-defined roles.
- Update user fields on the selected person record.
- Update user fields on accounts where the selected person holds institution-defined roles.
- Update card and/or electronic agreements related to the selected person record.

#1. Screen:
A new menu button is added under the 'More' menu in the DNA® Relationship Profile Screen. This button is enabled only when the user has proper authority and when the active customer record in the Relationship Profile screen represents a person. This process is not available for organizations.
Users can select the menu button to access the Fraud Lockdown screen, where they may choose to create or reverse a fraud lockdown for the customer active in the Relationship Profile screen. The Fraud Lockdown screen contains a drop-down selector to allow the user to choose the Fraud Lockdown to be processed and the tasks related to the chosen Lockdown Type is performed upon clicking the Process button.
For a Fraud Lockdown reversal, the most recent Fraud Lockdown type on the person is presented for reversal. No other reversal activity may be processed from this screen. The Fraud Lockdown performs only the tasks specified in the institution level variables under the variable type of *Custom Fraud Lockdown*. A person-level entity attribute '8FRDLCKDWN' is updated with the date and type of lockdown applied, which is further referenced by the custom screen in the event a reversal is initiated. The lockdown reversal uses the external interface cross-reference tables to determine the actions to be reversed for the given lockdown type.

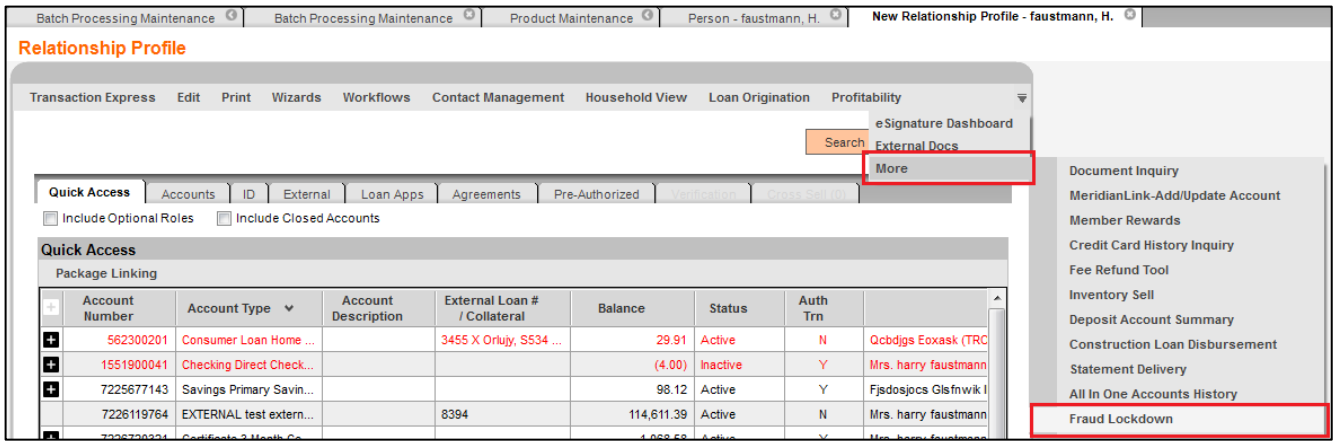
NOTE: If a user selects the incorrect Fraud Lockdown to be processed, the user should then reverse the Fraud Lockdown selected in error and then select the correct one to create.

Navigation:

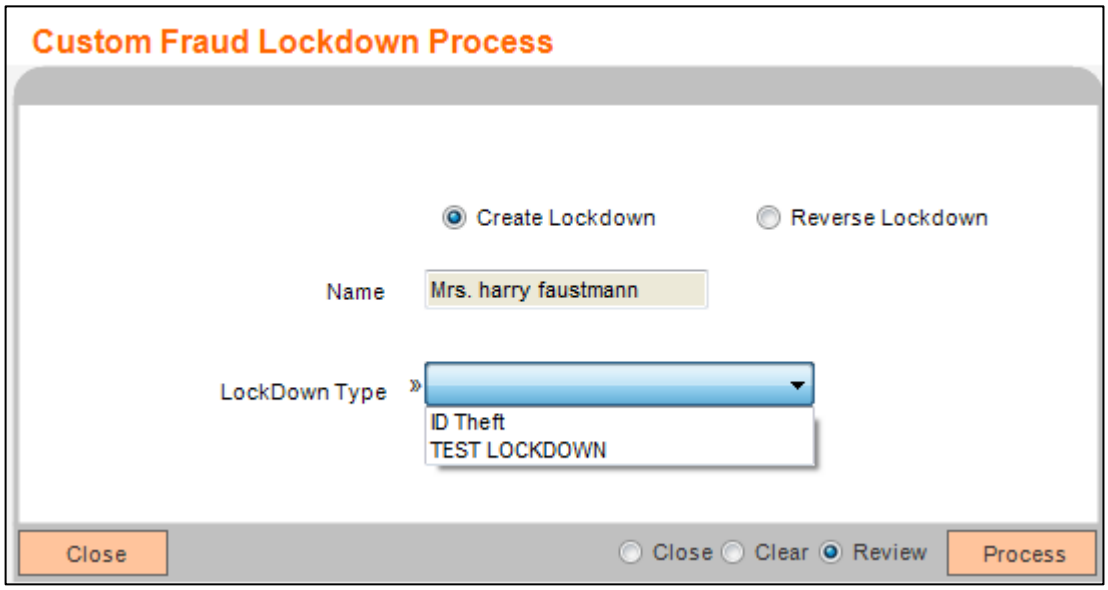
Relationship Profile > More > Fraud Lockdown

Screen Appearance:

A menu item ‘Fraud Lockdown ‘is displayed under the ‘More’ menu in Relationship Profile screen.



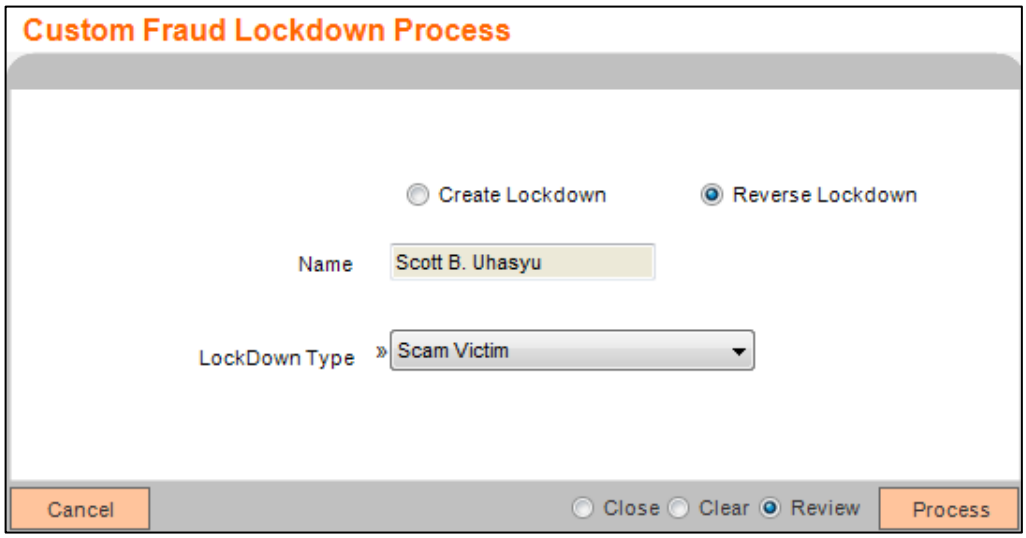
Upon selecting the Fraud Lockdown menu item, a screen is launched to select the Lockdown Type to be applied. The behavior for the chosen lockdown type is defined by the External Interface Cross Reference tables.



Field Listing:

Field	Description
Name	The name of the person is pre-filled and cannot be edited.
Create Lockdown	Radio button selector to select create lockdown
Reverse Lockdown	Radio button selector to reveres lockdown
Lockdown Type	Drop-down selector containing all valid Lockdown for selected person.

User is also able to reverse the lockdown, already applied on the person by selecting the 'Reverse Lockdown' radio button on the screen.



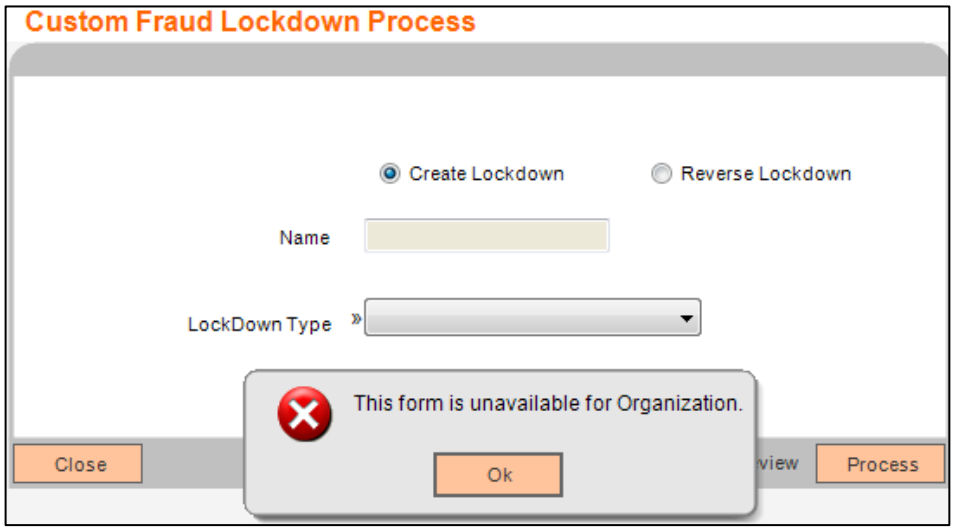
Authorization Item:
Access to this screen is controlled by a unique Authorization Item:

Authorization Item Code	Description
8FLP	Custom Fraud Lockdown Process

This Authorization Item needs to be linked to an Authorization Code (either an existing one or a new one created by the Financial Institution). Users with the Authorization Code will then have access to this functionality.

Messages:
The following Messages appears for client-side validations:

1) When organization is selected:



External Interface Cross Reference:
This solution uses the following External Interface Cross Reference variables to define the Fraud Lockdown types and their associated actions. An unlimited number of Fraud Lockdown types are defined through this method.

External Interface Category

External Interface Category Code	External Interface Category Description
8CSL	Custom Solutions Category

External Interface

External Interface Code	External Interface Description
8FLD	Fraud Lockdown

External Interface Variable

External Interface Variable Code	External Interface Variable Description	Description
8D01	Fraud Lockdown Type 01	Indicates the valid lockdown types for use with this process
8D02	Fraud Lockdown Type 02	Indicates the valid lockdown types for use with this process
8D03	Fraud Lockdown Type 03	Indicates the valid lockdown types for use with this process
8D04	Fraud Lockdown Type 04	Indicates the valid lockdown types for use with this process
8D05	Fraud Lockdown Type 05	Indicates the valid lockdown types for use with this process
8D06	Fraud Lockdown Type 06	Indicates the valid lockdown types for use with this process
8D07	Fraud Lockdown Type 07	Indicates the valid lockdown types for use with this process
8D08	Fraud Lockdown Type 08	Indicates the valid lockdown types for use with this process
8D09	Fraud Lockdown Type 09	Indicates the valid lockdown types for use with this process
8D10	Fraud Lockdown Type 10	Indicates the valid lockdown types for use with this process

External Interface Cross Reference

Variable Code	From Value	Description

	(Required Values for From Value)	
8D01	1 - Lockdown Type	The lockdown type to be applied This value is stored in a person level entity attribute at the time of the lockdown
8D01	2 - Lockdown Description	The description appears for this lockdown type in the custom screen drop-down selector
8D01	3 - Person Flag 1	The warning flag code to be applied for restricted person records (only one value accepted)
8D01	4 - Person UF1	User field code to be updated for restricted person records (only one value accepted)
8D01	5 - Person UF1 Value	The value to be written to the user field specified for value 'Person UF1'
8D01	6 - Person UF2	User field code to be updated for restricted person records (only one value accepted)
8D01	7 - Person UF2 Value	The value to be written to the user field specified for value 'Person UF2'
8D01	8 - Person UF3	User field code to be updated for restricted person records (only one value accepted)
8D01	9 - Person UF3 Value	The value to be written to the user field specified for value 'Person UF3'
8D01	10 - Acct Flag 1	The warning or lockout flag code to be applied to accounts where the restricted person holds a role as specified in the 'Acct Roles' value (only one value accepted) Note: In the event that both a warning flag and lockout flag exist with the same code, this process will apply lockout flags
8D01	11 - Acct Flag 2	The warning or lockout flag code to be applied to accounts where the restricted person holds a role as specified in the 'Acct Roles' value (only one value accepted) Note: In the event that both a warning flag and lockout flag exist with the same code, this process will apply lockout flags
8D01	12 - Acct Roles	Comma-separated list of Account Role Codes. The additional account roles for which to apply 'Acct Flag 1' and 'Acct Flag 2'. Tax owned accounts will always be included.
8D01	13 - Restriction Account Note Type	Comma-separated Note Class Code and Note Sub Class Code. The account note type and subtype to be placed for restricted accounts
8D01	14 - Restriction Account Note Text	The account note text for restricted account notes
8D01	15 - Major Types to Exclude	Comma-separated list of major account types for which the account-level flags should not be applied. If any major account type is listed in this value, restrictions will not be applied to ANY minor type within the given major. For example, to exclude all Consumer Loans from restriction, enter CNS in this value. To exclude only specific consumer loans from restriction, do not enter CNS here and enter the excludable minors in the Minor Types to Exclude value.

8D01	16 - Minor Types to Exclude	Comma-separated list of minor account types for which the account-level flags should not be applied. This value is used only to exclude minor types whose major account type has not be listed in the Major Types to Exclude.
8D01	17 - Agreement Types to Restrict	Comma-separated list of Agreement Type Codes. The agreement type codes to be updated for restricted person records. Note: If the Agreement Type Code is electronic, the application ignores the 18 - Agreement Status for Lockdown and 19 - Agreement Status for Reverse since electronic agreements do not have agreement statuses.
8D01	18 - Agreement Status for Lockdown	The Card status code to apply for agreements to be restricted for lockdown (Note: Only cards with a status of Active or Issued are eligible to be changed) (only one value accepted)
8D01	19 - Agreement Status for Reverse	The Card status code to apply for agreements to be restricted for lockdown reverse (Note: Only cards that have a status equal to the '18 - Agreement Status for Lockdown" value are eligible to be changed and where the previous status was ACT – previous card ISS status remain restricted) (only one value accepted)
8D01	20 - Agreement Status Comments	The status comments (Card Status Reason Code) to apply for restricted agreements (only one value accepted)

Configuration Checklist:

Item	**Test Environment**	**Production Environment**
External Interface Cross Reference		
Authorizations		

#2. Processing - PS_FRAUD_LOCKDOWN:

This application accompanies this process by producing a report of all lockdowns and lockdown reversals initiated through the custom screen for the given time period. It also optionally produces a comma-separated file mirroring the report data.

Parameters:

Parameter	Code	Description (how used)	Required	Default
Start Date	SD	Beginning date for which to report automated fraud lockdown activity.	No	Queue Effective Date
Thru Date	TD	Ending date for which to report automated fraud lockdown activity.	No	Queue Effective Date
Create Secondary Report	SRYN	Y = Create comma-separated file containing report data N = Do not create comma-separated file	No	N

Parameter	Code	Description (how used)	Required	Default
Output File Path	COUP	When Create Secondary Report = Y, complete path name where output file should be written. The trailing backslash is optional (ex. “C:\TEMP\ “	No	Batch Queue Output Directory
Output File Name	COUF	When Create Secondary Report = Y, name of output file.	No	PS_FRAUD_LOCKDOWN.csv

Person Entity Attribute:

Attribute Name	Value
8FRDLCKDWN – Fraud Lockdown	Holds the type of Lockdown applied on a day

Activity:

This process updates activity, using the following Activity Categories and Activity Types

Activity Category	Code	Activity Type	Code	Activity Subject
Account Maintenance	AMNT	Account	ACCT	Account
Person Maintenance	PMNT	Person	PERS	Person

Report:

```
Bank:    Test Institution                                   Fraud Lockdown                                   Run Date:  07-30-2019
Report:  PS_FRAUD_LOCKDOWN                                                                                 Post Date:  07-30-2019

Queue Number      :  78655                                                                                  Run Time:  11:56:32
Application Number:  15904                                                                                  Cash Box:
Queue Sub Number  :  2                                                  SCHEMA
                                                                       OSIBANK

                                                                   DATABASE NAME
                                                                     CS14.WORLD

                                                                      RELEASE
                                                                    DNA 4.5.1.0

                                        07-30-2019 09:25:01 PM 269989 G:\OSI\BANK\SQT\4510\BAT_EXE\PS\


                                                                 REPORT PARAMETERS

                    Create Secondary Report:  Y
                    Output File Name:  PS_FRAUD_LOCKDOWN.csv
                    Output File Path:
                    StartDate:  07-07-2019
                    ThruDate:  07-30-2019
Bank:    Test Institution                                   Fraud Lockdown                                   Run Date:  07-30-2019
Report:  PS_FRAUD_LOCKDOWN                                                                                 Post Date:  07-30-2019
                                                                                                                Page:  1 of 1

Person Name           Pers Number  Account Number  Acct Role       MJCD/MICD  Agree Number  AgrTyp  Resp Person   Resp Pers Name

Harry Faustmann             3617       562300201  OWN             CNS/HELN        5250630  WWW                1  John Banker
                                    1002020081   TAX             CK/PL08         5250630  WWW
                                    1551900041   TAX             CK/PL27         5250630  WWW
                                    7225677606   TAX             CNS/FLAT        5250630  WWW
                                    7226119764   OWN/TAX         EXT/TEST        5250630  WWW
                                    7227511589   TAX             EXT/VIBS        5250630  WWW
                                    7227514624   TAX             MTG/10AM        5250630  WWW
                                    7227514632   TAX             MTG/10AM        5250630  WWW
                                    7227514640   TAX             MTG/10AM        5250630  WWW
                                    7227514658   TAX             MTG/10AM        5250630  WWW
                                    7227514666   TAX             MTG/10AM        5250630  WWW
                                    7227514674   TAX             MTG/10AM        5250630  WWW
                                    7227516597   TAX             EXT/LPS         5250630  WWW
Scott Uhasyu                3619         1002220  TAX             SAV/PL01        5250650  WWW                1  John Banker
                                    7200151427   OWN             EXT/VPLT        5250650  WWW
                                    7216106656   TAX             EXT/VISA        5250650  WWW
                                    7226394689   TAX             EXT/CENL        5250650  WWW
                                    7226394746   TAX             EXT/CENL        5250650  WWW
                                    7226394754   TAX             EXT/CENL        5250650  WWW
                                    7226394788   TAX             EXT/CENL        5250650  WWW

                                    7226665684   TAX             EXT/CENL        5250650  WWW
                                    7226721006   TAX             EXT/CENL        5250650  WWW
                                    7227524334   TAX             CNS/DLAC        5250650  WWW
                                    7227526934   TAX             EXT/CENL        5250650  WWW
Tcjnw Eegncq               18744         5935700  TAX             SAV/PL01        2628633  ATM                1  John Banker
                                                                                   5261539  WWW
                                    7227353569   TAX             EXT/VGLD        2628633  ATM
                                                                                   5261539  WWW
Tyqegrsd Eehswhe           20175         6149200  TAX             SAV/PL01        2629019  ATM                1  John Banker
                                                                                   5262437  WWW
                                    7227459820   TAX             EXT/VGLD        2629019  ATM
                                                                                   5262437  WWW
Aquuvo Edywsy              21586                                                                                1  John Banker

Total Person Processed: 5
```

Output report is sorted on Person Number.

File Layout:

Output File Layout – Comma Separated

Field	Field Name	Format	Description
1	Person Name	String	Customer Name
2	Person Number	Number	Customer person number
3	Account Number	Number	Account Number Updated
4	Account Role	String	Customer Role Code on the given account
5	Major Account Type	String	Major Account Type Code
6	Minor Account Type	String	Minor Account Type Code

Field	Field Name	Format	Description
7	Agreement Number	Number	Agreement Number Updated
8	Agreement Type	String	Agreement Type Code
9	Responsible Person	Number	Person Number who performed lockdown

Additional Requirements:

- DNA 4.4.2 or later version is required.
- Core API 1.4.1 or higher (available for download from the Extranet at http://extranet.opensolutions.com/Lists/Downloads/Core%20API.aspx)
- The Relationship Profile More Menu DNAapp needs to be installed prior to installing this DNAapp

Configuration Checklist:

Item	Test Environment	Production Environment
Parameters		
External Interface Variables		

Installation:

1. Install the application through DNAapp Management Console (formerly known as DNA Configuration Toolkit). The instructions on how use the DNAapp Management Console is delivered along with the DNAapp Management Console. Please contact Client Care if you need assistance using the DNAapp Management Console.

2. Client Side dll files:
   a. PS_FraudLockDown.Business.dll
   b. PS_FraudLockDown.Screen.dll

   for this application should be placed at each branch server in the following path:

   X:\OSI\DNA_Client\DNAApps\9999\Bin

   Where:
   X = drive mapping for the branch server the DNA client is located on
   9999 = the current DNA release

Revisions:

Date	App Version #	Change
07/2023	1.0.1.2	Recompile the package
05/2023	1.0.1.1	Modified the API to always create a new note number when applying lockdown unless the same employee previously applied a lockdown on the same post date (API was getting any note matching the fraud lockdown text regardless of the create person).

Date	App Version #	Change
04/2022	1.0.1.0	Added lockdown for electronic agreements; Expanded LockDown Description from 60 to 256 (ToValue column width); Modified Person Roles for account Lockouts/warnings by linking notenbr; Changed getting noteNbr by not using createpersnbr since the person reversing the lockdown may not be the one who applied the lockdown; Added electronic agreement activity to batch application; Added ISS card status when restricting card agreements (when reversed, the previously ISS cards do NOT become Active).
02/2022	1.0.0.16	Modified to accept a <LockDownTyp> value of up to 60 characters from 30 characters to resolve Oracle error ORA-06502: PL/SQL: numeric or value error: character string buffer too small; Modified selection of accounts for lockouts/notes to populate when 15 - Major Types to Exclude and 16 - Minor Types to Exclude have null values
06/2021	1.0.0.15	Modified External Interface Category 8CST to 8CSL.
05/2021	1.0.0.14	Modified to correct previous update “Only update Card Status when reversing lockdown and previous Card Status is Active”
05/2021	1.0.0.13	Modified to correct previous updates “Only update Card Status when reversing lockdown and previous Card Status is Active” and “Updated Install and Uninstall scripts to replace External Interface Category of 8CSL to 8CST”
05/2021	1.0.0.12	Updated Install and Uninstall scripts to replace External Interface Category of 8CSL to 8CST.
05/2021	1.0.0.11	Core API package changes only: Modified to: Only update Card Status Reason Code with 20 - Agreement Status Comments and Card Status Reason and Status Reason (Comments from front end) with the Code description; Only update Cards Status Reason information for creation of lockdown (previously updating for reverse of lockdown; Only update Card Status when creating lockdown and Card Status is Active; Only update Card Status when reversing lockdown and previous Card Status is Active;
04/2021	1.0.0.10	Updated Install and Uninstall scripts to replace External Interface Category of 8CSL to 8CST. Core API package: Modified Exclude Major/Minor for person with designated roles so that major/minors that are excluded are excluded.
04/2021	1.0.0.9	Core API package changes only: Added Major/Minor exclusion to TRO owned accounts (was only excluding for Role accounts); Changed the Create Person from the person being locked down to the DNA user person; Added CreateDateTime to Note insert; Added Card Status Reason (Comments) to main select so that if there is an invalid 20 - Agreement Status Comments value, the Card Member Issue History will still get updated for other values (was not inserting if invalid Card Status Reason (Comments);

Date	App Version #	Change
		Added Card Status to main select so that if there is an invalid 19 - Agreement Status for Reverse value, attempt to update Card Member/Card Member Issue History would not take place; When creating fraud lockdown only update Card Member/Card Member Issue History when ACT/ISS card statuses; When reversing fraud lockdown only update Card Member/Card Member Issue Hist when status is equal to 18 - Agreement Status for Lockdown (when the lockdown took place); Added Status to Card Member Issue History insert
09/2020	1.0.0.8	Validation findings fixed; added minimum required Core API version and attribute 8FRDLCKDWN in user document
08/2020	1.0.0.7	Corrected ExtIntfVarDesc of code 8D07
07/2020	1.0.0.6	Screen Only: Modified User Authentication to support Citrix environment
07/2020	1.0.0.5	Removed Public Synonym script as Configuration Toolkit creates the public synonym from API DNAX
06/2020	1.0.0.4	Corrected API DNAX by removing CreateRowTyp (not required for pl/sql) and removed commit thereby eliminating installation script error
06/2020	1.0.0.3	Repackaged for changes to 15972 FraudLockdown API (Rewrote to support multiple Lockdown Types, perform updates using pack_ps_common.) and added the 8CSG CAPI installation to set Cashbox Pooling to N at the application level.
02/2020	1.0.0.2	Corrected update for Agreement Status Comments
01/2020	1.0.0.1	Clarified 18 - Agreement Status for Lockdown and 19 - Agreement Status for Reverse descriptions in document. Repackaged for changes to 15972 FraudLockdown API
07/2019	1.0.0.0	Application Created