

# NCR Aloha Takeout

## How ATO Handles PII Data Privacy

Last Updated: March 5, 2019

first name?

last name?

phone number?

address?

latitude?



longitude?

email address?

city?

zip code?

company?

### What is PII Data?

Personally Identifiable Information (PII) is any sensitive or non-sensitive data that can potentially identify, contact, or locate a specific individual. PII can be exploited by criminals to stalk, steal the identity of, or simply to invade the privacy of an individual. Several laws, enacted by various countries, provide regulations for safeguarding PII data, and a violation for exposing such information can lead to fines and potential imprisonment.

While each Aloha-centric product continually makes improvements to enhance the merchant-to-guest experience, you must keep such information secured and not available to unauthorized persons or entities. In addition, you must make PII data from some third-party partners unusable in a way that makes it impossible to identify the guest as soon as the system no longer requires the data for order fulfillment.

This document describes how Aloha Takeout® (ATO) handles sensitive PII data to comply with regulations. To meet each need, ATO addresses several issues:

- ATO must ensure that any means used by an attacker or a third-party partner to retrieve PII data for use outside of the product is cost-prohibitive.
- While secured, PII data must still be usable for searching and querying records and information.
- You must still be able to display and or print the unencrypted PII data, when required for business purposes.
- You must be able to relate an order to a guest even after the system alters PII data.

### Terms Used in This Document

Glossary Term	Description
Encryption	A masking process that makes data usable to authorized personnel only.
Fuzzy search	Returns a list of results based on likely relevance even though search words and spellings may not exactly match.
Hash	Transforming a string of characters into a usually shorter fixed-length value or key that represents the original string.
Like search	Allows using wildcard characters to search.
Order aggregator	A third-party intermediary who collects orders and fulfills the guest order.
Obfuscation	The process of replacing original data with random characters in view or print mode.
Order fulfillment	Order life span from order inception to delivery.
Personally identifiable information (PII) data	Information used to uniquely identify, contact, or locate a specific individual, company, or entity or that can combine with other sources to uniquely identify an individual, company, or entity. Data such as name, address, and phone number are examples of PII data.
Salt	Random data used as an additional input to a one-way function that hashes data, a password, or passphrase. Used to safeguard passwords in storage. The system randomly generates a new salt each time the data passes through the system.

# How ATO Handles PII Data Privacy

## Encrypting and Obfuscating PII Data

The system must secure PII data when not actively in use. To ensure this, ATO uses a combination of encryption and obfuscation to protect the data.

### Encryption

ATO encrypts PII data before storing the information into its database, and decrypts it when reading the data back into memory. In addition, for certain operations, screens, documents, or other artifacts, ATO determines whether to use/display/print encrypted or unencrypted PII data.


ATO uses the same library and keys to encrypt PII data and other sensitive information; however, the process differs because the security requirements around sensitive data are much more stringent than those related to PII data. The encryption method ATO uses for PII data includes salting the key each time PII data gets transmitted, so that sending the same information twice results in distinctly different encrypted values. This prevents attackers from deciphering information by sending in the same data multiple times.

### Obfuscation

In certain circumstances ATO obfuscates PII data upon order fulfillment. This occurs when the system removes PII data from the historical tables and the Aloha Takeout End-of-Day (EOD) process clears active data. The system replaces PII data with hashes, using the SHA-512 algorithm, which is then treated as normal PII data. This allows ATO to determine information without the ability to uniquely identify, contact, or locate the guest. Metrics such as 'how many unique guests ordered a specific item' or 'how much did a guest spend at a specific store' can be collected and measured while protecting PII data.

Our API obfuscates data when sending to ATO. Data that you manually enter into ATO is not obfuscated. The following rules provide the guidelines for obfuscation:

- The order data object has a Boolean value called `ObfuscatePiiDataUponOrderFulfillment`.

 *Development is required on the Ordering Essentials and ODSP APIs to support this feature.*

If the value = True, ATO obfuscates the PII data for the order upon order fulfillment regardless of other settings or options.


If the value = False (default) the remaining rules govern whether to obfuscate the PII data for the Order.

- ATO obfuscates PII data upon order fulfillment, by default, if the order source on the order is an Order Aggregator.
- Each order source (including Order Aggregators), has an enumerated value called `ProtectPIIData`, which can have three possible values:

*Default* – ATO obfuscates PII data for this order, if the order source is in the list of Order Aggregators.

*NeverObfuscate* – ATO does not obfuscate PII data for this order regardless of the order source.

*AlwaysObfuscate* – ATO obfuscates PII data for this Order regardless of the order source.

 *The order level option, 'ProtectPIIData' takes precedence over the source default and/or configured value.*


## Using the Database

ATO must maintain the ability to perform fuzzy or 'like' searches as well as 'exact match' searches of PII data; however, the PII data stored in the database is encrypted, which can complicate such searches.

A fuzzy or 'like' search uses partial criteria and retrieves all records containing that criteria. For example, if you perform a fuzzy search for 'John,' the database returns all records where the first name, last name, or company name start with the letters 'John,' such as 'John,' 'Johnson,' 'Johnsonville,' and more.

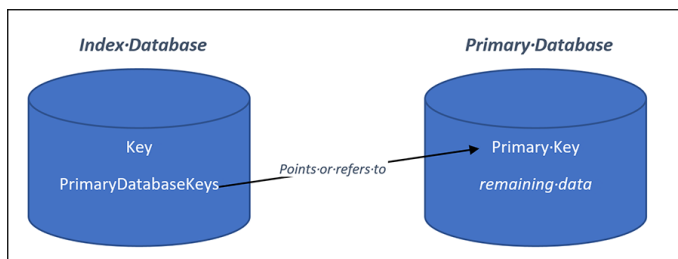
An exact match search retrieves the data for all records that exactly match the search criteria. For example, if you perform an 'exact match' search on 'John,' the database returns records where the first name or last name is 'John.' The search does not return records such as 'Johnson' or 'Johnsonville.'

Because ATO salts the encrypted data each time it transmits, you cannot encrypt the incoming search data and then perform an exact match search on the resulting encrypted value. Fuzzy searches become even more difficult to accomplish with encrypted data. To solve this problem, ATO stores and maintains an index of records inside an encrypted SQLite database, which means ATO encrypts the entire database. SQLite handles the encryption and search process within the database engine, thus removing the requirement for ATO to handle these processes. To prevent performance issues, it is not prudent to store the entire ATO database within an encrypted SQLite database. You store the encrypted index instead.

 *Any search excludes obfuscated data, but searches on parts of the record that are not obfuscated may still return records with obfuscated data.*

## Storing Indexes in Encrypted SQLite Database

ATO utilizes an encrypted SQLite database (hereafter referred to as the Index database) to facilitate data searching while ensuring that PII data remains encrypted. The records in the Index database point to the actual records in the Primary database in SQL Express or SQLite.



In this way, ATO connects the Index database to the Primary database while retaining the ability to prevent PII data from appearing in search results.

The Index database comprises one or more tables (one table per index) using the following structure:

Column Name	Column Type	Purpose
Key	Varchar Primary Key	The key value for the record in the Index database.
Primary Database Key	Varchar	A delimited list of values which are the primary key for the associated record in the Primary database.

## ATO Specific Database Implementation

ATO utilizes the Index database to facilitate searches for guest data. Currently, ATO holds guest data in the Guest, Address, and PhoneNumber tables in the Primary database. ATO allows you to search for a guest by first name, last name, phone numbers, or company name. To implement this, the Index database includes a GuestIndex table. The Index database contains a record for each unique first name, last name, phone number, and company name. If a record already exists, ATO appends the Primary database primary key value in the Index database.

## Searching the Database

From ATO you can search the database in two ways. The look-ahead function allows you to retrieve partial information. For example, you can search a partial string to return a list from which to select the specific record.

### To use the look-ahead function:

1. Type a **partial string** upon which to search. ATO searches the Key column in the Index database and compiles only the matching values into the search result.
2. Select a **specific record** from the list of matching values returned to ATO.


You can search an exact match record in the database and retrieve only the unencrypted information to identify a guest in connection with a specific order.

### To use the search function:

1. Type the **specific information** to search. ATO searches the Key column in the Index database and compiles only the matching values into the search result. This search result splits the values in the PrimaryDatabaseKeys column on the delimiter and provides a list of primary key values. The system then searches the Primary database primary key values and compiles the matching values into the search result to return to ATO.
2. Select the resulting **matching record**.

## Example Search Implementation

This example shows how different search criteria combine to produce useable, protected results.

 In the two example tables presented, the Row column does not actually appear in the table. We use it here for illustrative purposes only.

The Guest database splits data across multiple tables, so the data shown in the Primary database GuestIndex table example comes from multiple tables using the Guest table primary key as the common Key. Thus, ATO uses that value to perform the lookup on the Primary database.

### Primary database 'Guest' Table data:

Row	Primary Key	First Name	Last Name	Phone Number	Company Name
1	1	John	Smith	8881112222	Johns PC Repair
2	2	John	Morgan	8882223333	NCR
3	3	Frank	Johnson	3334445555	
4	4			8881112222	Ace Lawn Care
5	5	Morgan	James	6443228877	Johns PC Repair

### Index database 'GuestIndex' Table data

Row	Key	Data
1	John	1,2
2	Smith	1
3	8881112222	1,4
4	Morgan	2,5
5	8882223333	2
6	NCR	2
7	Frank	3
8	Johnson	3
9	3334445555	3
10	Ace Lawn Care	4
11	James	5
12	6443228877	5
13	Johns PC Repair	1, 5

## Example of a Fuzzy search:

You initiate a fuzzy search for 'John.' ATO searches the GuestIndex table in the encrypted Index database for any entries starting with 'John.' SQLite returns rows 1, 8, and 13.

Row 1 has the values '1' and '2' in the Data column, row 8 has the value '3' in the Data column, and row 13 has the values '1' and '5' in the Data column. The system then returns the results from the Data column to ATO in a list '1,' '2,' '3,' and '5.'

ATO searches the Primary database for all records containing the Primary Key value '1,' '2,' '3,' or '5.' SQL Express return rows '1,' '2,' '3,' and '5.' and the data in the Guest Table (first name, last name, phone number, and company name) for those rows is presented to the user.

## Displaying, Printing, Storing, Exporting and Transmitting PII Data

Many processes in ATO require PII data to appear, print, write to a file, or send across the network. For each process, ATO uses unencrypted PII data only when necessary. If not required, then ATO uses encrypted. The ATO team has identified the following processes that use PII data. Obfuscation of PII data occurs during the EOD process.

### Printing

Consumer PII required to fulfill order. Printing consumer PII on printable artifacts used to fulfill order.

**Encryption:** Data not encrypted.

**Obfuscation:** Data not obfuscated.

### Reporting

ATO reporting includes orders from aggregators; all PII for those orders protected.

**Encryption:** Data encrypted, if [ProtectPIIData = True].

**Obfuscation:** Data obfuscated, if reports run on historical data. Data not obfuscated, if reports run on active data; the encryption rule protects the data.

### Report exports

Report exports protect all PII data from aggregator consumers.

**Encryption:** Data encrypted, if [ProtectPIIData = True].

**Obfuscation:** Data obfuscated, if reports run on historical data. Data not obfuscated, if reports run on active data; the encryption rule protects the data.

### Data exports

ATO data export tools decrypt consumer PII owned by Aloha. All aggregator consumer PII data protected.

**Encryption:** Data encrypted, if [ProtectPIIData = True].

**Obfuscation:** Data obfuscated, if reports run on historical data. Data not obfuscated, if reports run on active data; the encryption rule protects the data.

### ATO database

All PII data encrypted in the ATO database. When PII for aggregator consumers moved to historical tables, the data is obfuscated and then encrypted following the standard encryption used for all other PII data.

**Encryption:** Data encrypted.

**Obfuscation:** Data obfuscated when the Aloha Takeout EOD runs, if data is set for obfuscation. Data not set for obfuscation, not obfuscated.

### On screen

Consumer PII used to fulfill the order. Showing consumer PII on screen, normal part of order fulfillment.

**Encryption:** Data not encrypted.

**Obfuscation:** Data not obfuscated.

### GCHKINFO

When adding consumer PII to guest check in Aloha, ATO adds encrypted data for PII for aggregator consumers.

**Encryption:** Data encrypted if [ProtectPIIData = True].

**Obfuscation:** Real time data not obfuscated; data protected by the encryption rule.

## Order Status Updates

ATO encrypts order status updated for orders from aggregators. PII data not encrypted or obfuscated when sending updates to Order Service,

**Encryption:** Data encrypted for ATO API if [ProtectPIIData = True]. Data not encrypted for Order Service Updates.

**Obfuscation:** Not Applicable. ATO provides no status updates for orders after EOD.

## ATO logs

ATO logs encrypted PII data for all orders.

**Out of Scope:** ATO creates a log tool that allows PII data to be decrypted for troubleshooting. All PII data from aggregators must be obfuscated prior to being encrypted and written to the log. Because aggregator PII data is obfuscated prior to encryption, using the tool to decrypt PII data shows only obfuscated PII data for aggregator orders. Before we create the log tool, we must obfuscate Aggregator PII prior to writing

## Aloha Check Name

**Encryption:** Data encrypted if [ProtectPIIData = True]. Non-protected data not encrypted.

**Obfuscation:** Because data is not obfuscated until EOD, obfuscation not in scope.

## Databus messages

Because fulfilling an order requires consumer PII data, PII data appears on screen in Aloha Kitchen (AK). AK then obfuscates order aggregator PII during EOD. AK considers the source of the order to determine whether to obfuscate the data. Another option is for ATO to provide a data element to AK to let it know to obfuscate PII at EOD.

**Encryption:** Data not encrypted.

**Obfuscation:** Data not obfuscated.

ATO passes the ProtectPIIData flag with the order, to tell the external application how to handle the data.

## ATO API (GetOrderStatus)

If a request is made and the return calls include PII data, ATO will validate if the order \ guest originated from an aggregator and return encrypted data in appropriate fields.

**Encryption:** Data encrypted if [ProtectPIIData = True].

**Obfuscation:** Because data is not obfuscated until EOD, obfuscation not in scope. Today, the get order status call does not return historical orders.

## Offline data files

All data is encrypted in ATO offline data files.

**Encryption:** Data encrypted.

**Obfuscation:** Because data is not obfuscated until EOD, obfuscation not in scope.