WATCHTOWER

BY LIGHTHOUSE

DATA SECURITY WHITE PAPER

How Watchtower Protects Your Client List

How we encrypt, store, screen and delete the information you give us.

OCTOBER 2026

Watchtower by Lighthouse is a service of Lighthouse Services USA, LLC · watchtowerkyc.com

Summary

Watchtower screens your clients against government sanctions lists and rosters of public office holders. To do that we hold your client list, and this paper sets out how we protect it.

- We encrypt every name, date of birth, nationality and file reference before it is written to the database.
- We encrypt every screening result that could identify a client.
- Your users sign in with passkeys, and we store no passwords.
- We screen on our own systems and send the names you screen to no outside screening service.
- Our staff have no screen that displays your clients.
- We log every sign-in, change and download, and your administrators can read and download the log.
- We delete your client list ninety days after your subscription ends, or earlier at your written request.
- If a breach affects your data, we tell you within forty-eight hours.

Information We Hold

We hold four kinds of information for each subscriber.

YOUR PARTIES	The people and entities you screen. For each one we hold the name, any former names and aliases, the date of birth, the nationality, your file reference and the party's role.
YOUR RESULTS	The result of every screening, the list entries and office holders that a party matched, and the decisions and reasons your compliance officer records.
YOUR ACCOUNT	Your firm's name and the names and email addresses of your users.
YOUR BILLING	Your plan and the amounts charged. You enter card details with Stripe, and we receive no card numbers.

Encryption at Rest

We encrypt sensitive fields with AES-256 in GCM mode before they are written to the database. The encryption is applied to the following fields:

- each party's name, former names and aliases, date of birth, nationality, file reference and role;

- the name and date of birth recorded with each screening result;
- the list entries and office holders that a party matched, including the name on each entry;
- the reasons your compliance officer records, and each standing decision that a match is a different person;
- the description on each audit log entry;
- the name, date of birth, nationality and email address entered for a single check.

A sanctions match is a match on a name, and the name on the list is therefore close to your client's name. For that reason we encrypt the list entries a party matched in the same way as the party's own details. Where the database has to find an earlier decision again, it stores a keyed hash of the party and of the list entry.

So that a large book can be searched, the database also stores a keyed hash of each word of a party's names and of your file reference. A person who obtained a copy of the database without the key could see that two parties share a word and how often a word occurs. That person could not see what the word is.

The database holds a small number of fields in clear because it has to sort and count by them. These are the firm that a record belongs to, whether a party is a person or an entity, the dates of screening, and whether a result is Clear, Review or Match. A person who obtained a copy of the database would see those fields beside encrypted names, dates of birth, nationalities and references.

We hold the encryption key in the hosting platform's secret store, which is separate from the database. The database host then encrypts the database a second time.

Encryption in Transit

Every connection to Watchtower is encrypted with TLS, and browsers are instructed to refuse an unencrypted connection to the site for two years at a time. The site instructs browsers that no other site may display it in a frame, and that it may load scripts only from Watchtower and from the service that guards its contact form.

Sign-In

Your users sign in with a passkey that is held on the user's own device and confirmed by fingerprint, face or device PIN. We store no passwords, which removes the most common way accounts are stolen.

- Only an administrator at your firm can invite a user. The invitation link works once and expires after seventy-two hours.
- A session ends after thirty minutes without activity.

- We hold sessions on the server, and a user who signs out or is deactivated loses access immediately.
- The session cookie is sent only over an encrypted connection and cannot be read by scripts on the page.

Separation of Subscribers

Each subscriber's records are marked with that subscriber's identity. Every request for those records passes through a single part of the software, which takes the subscriber's identity from the signed-in session and adds it to the request.

We check this automatically before each release. The release is stopped if any other part of the software reaches the database directly, if a request for a subscriber's records omits the subscriber's identity, or if a page behind sign-in fails to confirm the user before it answers. We also run a test that requests every kind of record under a false subscriber identity and confirms that no record of another firm is returned.

Import

When you import an Excel workbook, your browser reads the file and sends only the rows to Watchtower over the encrypted connection. We check each row, show you what will be imported, and keep only the parties you confirm.

When you import a Google Sheet, you share the sheet with Watchtower as a viewer and we read it once. You can remove that access as soon as the import is complete.

Screening

We download the sanctions lists and the rosters of public office holders from their publishers and compile them on our own systems. We compare your parties against them on those same systems. We send the names you screen to no list publisher, data vendor or outside screening service.

Stripe receives your billing details and your plan when you pay. We send Stripe no information about the parties you screen.

Access by Lighthouse Staff

Our staff have no screen that displays a subscriber's parties or results. The staff who run the service work on its systems, where your client information is held encrypted. The alerts our staff receive carry counts and reference numbers and no client names.

We use the details of the parties you screen for one purpose, which is to run the screening you ordered and to issue the certificates and reports to you. We hold those details apart from the records of every Lighthouse company's own clients, and we do not use them to approach or to serve any party you screen.

Audit Log

We write an entry to your audit log for each of the following events:

- a sign-in or a failed sign-in;
- a party added, imported or changed;
- a screening run;
- a review decision;
- a certificate, report or audit log downloaded;
- a user invited or deactivated;
- a change to your screening schedule.

Each entry records the user and the time. Your administrators can read the log in the account and can download the whole log as a PDF or as a CSV file.

Certificates and Reports

Each certificate and report states the date and time of the screening, the lists and rosters it was run against, and the result, and each carries a reference number. We build every document from the stored record of the screening, and a copy issued later is identical to the first.

We issue certificates, reports and the audit log as locked PDF files, which can be read and printed and cannot be edited in a PDF reader. Your users download them from the account after signing in. The email that tells your administrators a screening has run carries the counts and a link to the account.

Retention and Deletion

We keep your information for as long as your subscription runs. Ninety days after it ends we delete your account and all of its users, passkeys, parties, results, decisions and audit log entries. You can sign in during those ninety days to read and download your records, and you can ask us in writing to delete them earlier.

We delete the details entered for a single check ninety days after payment, and after one day if the check is not paid for. We keep billing records for the period the law requires.

Location and Service Providers

The service is hosted in the United States, and the information you submit is held there. We share information only with the companies that host the service, deliver its email and process its payments, and each of them may use it only to provide that service to us. We do not sell information, and we do not share it for advertising. The website carries no advertising or tracking cookies.

Independent Review

We work with Scytalex LLC, a security firm that audits our security practices and helps harden the service.

Breach Notice

If a breach affects your data, we tell you within forty-eight hours. We tell you what happened and which information was affected, so that you can notify your own clients and regulator.

Contact

We answer questions from your compliance officer, your information security team and your regulator, and we complete security questionnaires. Please write to support@watchtowerkyc.com.