CLAIMS

We claim:

1. A system for automatically verifying and monitoring digital records, comprising:

a digital processor;

a computer readable medium comprising executable instructions that, when executed, cause the system to automatically execute a verification process and a monitoring process for verifying and monitoring digital records including licenses and certifications;

wherein the verification process comprises the following steps:

generating a display requesting certification information;

receiving certification information;

generating a display requesting third party authorization;

receiving third party authorization;

searching for member certification records in member certification database;

determining whether or not there is a match;

submitting member certification information to an applicable certifying organization;

receiving member certification status from certifying organization; and

determining whether or not certification is valid; and

wherein the monitoring process comprises the following steps:

receiving a verification request from a customer, the verification request including defined search criteria, including a credential holder name and identifier, wherein the verification request is received via a web-based dashboard interface or an application programming interface (API);

requesting input data from the customer to ensure an accurate match;

assigning a unique number to the verification request and queuing the verification request for processing by a distributed verification engine, wherein the distributed verification engine is programmed to search for and identify the next verification request in queue and automatically execute the verification process on the next verification request;

aggregating both structured and unstructured verification data without human intervention; and

determining whether the credential is valid, active, expired, or includes a discrepancy.

2. The system of claim 1, wherein the verification process further comprises the following steps:

if no valid member certification record is determined, insert the member certification record into the member certification database with a flag denoting that the certification is not valid and will not display the member certifications;

if a valid member certification record is found, insert the member certification record into the member certification database;

upon successful insertion of the valid member certification record, transmit a message to display the valid member certification information.

3. The system of claim 1, wherein the monitoring process further comprises the following steps:

capturing all metadata associated with the verification, the metadata including data representing an expiration date, address, adverse actions, and/or disciplinary actions;

automatically capturing a screen shot of the certification organization's website to provide a visual record of what the system encountered when it captured the verification, and making the screenshot available in a verification history for each verification processed; and

adding the data results to the credential holder’s profile history.

4. The system of claim 1, further comprising adding verification results to a blockchain distributed ledger, thereby providing an unalterable audit log.

5. The system of claim 3, further comprising providing automatic notifications based on status, including change of status from active to expired, active to suspended, or active to revoked.

6. The system of claim 2, wherein the monitoring process employs customizable triggers and alerts to provide notifications for change in status or pre-expiration of a license or certification being monitored.

7. The system of claim 6, wherein the change in status of a license or certification being monitored includes one or more of: normal expiration, disciplinary action, administrative action, revocation, and pre-expiration.

8. The system of claim 1, wherein the system further comprises instructions that, when executed, cause the system to execute a process to simulate a browser visiting a website of an external web-based system, submitting requests, and parsing returned data to capture data pertinent to licenses and certifications maintained by the external web-based system.

9. The system of claim 8, wherein the external web-based system provides information via form submissions but does not make available an application programming interface (API) suitable to capture data.

10. The system of claim 1, wherein the system further comprises instructions that, when executed, cause the system to employ blockchain technology to make verification data part of a distributed ledger, thereby creating an unalterable audit log of all of verifications processed.

11. The system of claim 10, wherein the audit log provides a globally searchable database of individuals and their licenses that outputs a verification stored in the blockchain.

12. The system of claim 1, wherein the system further comprises instructions that, when executed, cause the system to execute a CSV import process to create a comma separated values file in a correct format for bulk uploads depending on user selected verification types.

13. A process for automatically verifying and monitoring digital records, comprising:

a verification process for verifying digital records including licenses and certifications; and

a monitoring process for monitoring said licenses and certifications;

wherein the verification process comprises the following steps:

generating a display requesting certification information;

receiving certification information;

generating a display requesting third party authorization;

receiving third party authorization;

searching for member certification records in member certification database;

determining whether or not there is a match;

submitting member certification information to an applicable certifying organization;

receiving member certification status from certifying organization;

determining whether or not certification is valid;

if no valid member certification record is determined, inserting the member certification record into the member certification database with a flag denoting that the certification is not valid and will not display the member certifications;

if a valid member certification record is found, inserting the member certification record into the member certification database; and

upon successful insertion of the valid member certification record, transmitting a message to display the valid member certification information.

14. The method of claim 13, wherein the monitoring process comprises the following steps:

receiving a verification request from a customer, the verification request including defined search criteria, including a credential holder name and identifier, wherein the verification request is received via a web-based dashboard interface or an application programming interface (API);

requesting input data from the customer to ensure an accurate match;

assigning a unique number to the verification request and queuing the verification request for processing by one of a distributed verification engine, wherein the distributed verification engine is programmed to search for and identify the next verification request in queue and automatically execute the verification process on the next verification request;

aggregating both structured and unstructured verification data without human intervention;

determining whether the credential is valid, active, expired, or includes a discrepancy;

capturing all metadata associated with the verification, the metadata including data representing an expiration date, address, adverse actions, and/or disciplinary actions;

automatically capturing a screen shot of the certification organization's website to provide a visual record of what the system encountered when it captured the verification, and making the screenshot available in a verification history for each verification processed; and

adding the data results to the credential holder’s profile history.

15. The method of claim 13, wherein the monitoring process employs customizable triggers and alerts to provide notifications for change in status of a license or certification being monitored, wherein the change in status includes normal expiration, disciplinary action, administrative action, revocation, or pre-expiration.

16. The method of claim 13, wherein the method further comprises a process to simulate a browser visiting a website of an external web-based system, submitting requests, and parsing returned data to capture data pertinent to licenses and certifications maintained by the external web-based system.

17. The method of claim 16, wherein the external web-based system provides information via form submissions but does not make available any application programming interface (API).

18. The method of claim 13, wherein the method further comprises a process to employ blockchain technology to make verification data part of a distributed ledger, thereby creating an unalterable audit log of all of verifications processed.

19. The method of claim 18, wherein the audit log provides a globally searchable database of individuals and their licenses that outputs a verification stored in the blockchain.

20. The method of claim 13, wherein the method further comprises a CSV import process to create a comma separated values file in a correct format for bulk uploads depending on user selected verification types.

21. A computer readable medium comprising executable instructions, that, when executed, cause the system to:

execute a verification process for verifying digital records including licenses and certifications; and

execute a monitoring process for monitoring said licenses and certifications;

wherein the verification process comprises the following steps:

generating a display requesting certification information;

receiving certification information;

generating a display requesting third party authorization;

receiving third party authorization;

searching for member certification records in member certification database;

determining whether or not there is a match;

submitting member certification information to an applicable certifying organization;

receiving member certification status from certifying organization;

determining whether or not certification is valid;

if no valid member certification record is determined, inserting the member certification record into the member certification database with a flag denoting that the certification is not valid and will not display the member certifications;

if a valid member certification record is found, inserting the member certification record into the member certification database; and

upon successful insertion of the valid member certification record, transmitting a message to display the valid member certification information; and

wherein the monitoring process comprises the following steps:

receiving a verification request from a customer, the verification request including defined search criteria, including a credential holder name and identifier, wherein the verification request is received via a web-based dashboard interface or an application programming interface (API);

requesting input data from the customer to ensure an accurate match;

assigning a unique number to the verification request and queuing the verification request for processing by one of a distributed verification engine, wherein the distributed verification engine is programmed to search for and identify the next verification request in queue and automatically execute the verification process on the next verification request;

aggregating both structured and unstructured verification data without human intervention;

determining whether the credential is valid, active, expired, or includes a discrepancy;

capturing all metadata associated with the verification, the metadata including data representing an expiration date, address, adverse actions, and/or disciplinary actions;

automatically capturing a screen shot of the certification organization's website to provide a visual record of what the system encountered when it captured the verification,

and making the screenshot available in a verification history for each verification processed; and

adding the data results to the credential holder's profile history.