Employer's Guide to State Biometric Privacy Laws

Statues, Penalties and Best Practices for Compliance and EPAY Systems' Policies and Procedures

EPAY SYSTEMS

SEYFARTH SHAW LLP ATTORNEYS

About Seyfarth Shaw

With more than 900 attorneys and 15 full-service offices in the United States, London, Shanghai, Hong Kong, Melbourne, and Sydney, Seyfarth Shaw LLP offers a national platform and an international gateway to serve our clients' changing business and legal needs in corporate, employee benefits, employment, litigation, and real estate. Our clients range from *Fortune* 100 to midsize companies, and include publicly traded and privately held companies and various types of funds.

Our client-first approach has resulted in numerous accolades from a variety of highly respected industry associations, consulting firms, and the media. In its 2017 report, Seyfarth has been named by BTI Consulting to its Client Service A-Team for the 7th straight year. In 2017, our Labor & Employment Department was recognized by Chambers as a Band 1 firm nationwide; we were also shortlisted in the Labor & Employment category for the prestigious 2017 Chambers USA "Award for Excellence." Law360 named Seyfarth Employment Group of the Year in 2016.

Attorneys

Noah Finkel is a partner in the Labor & Employment Department and is a Co-Chair of the Wage & Hour Litigation Practice Group in Seyfarth's Chicago office. Mr. Finkel is one of three editors-in-chief of the treatise Wage & Hour Collective and Class Litigation, a more than 1,000-page book devoted to the litigation of wage & hour matters. The treatise literally is "the book" on wage & hour litigation.

Thomas Ahlering is an associate in the Chicago office of Seyfarth Shaw LLP and a member of the firm's Labor & Employment Department. Mr. Ahlering represents some of the world's largest corporations in litigation with millions of dollars at stake in a broad range of employment disputes, including defending employers against claims under the the Illinois Biometric Privacy Act.

Mr. Ahlering brings a unique perspective to defense teams as a former class action plaintiff lawyer and his experience on both sides of the aisle in class action litigation provides him with the ability to see all sides of a case and to anticipate and defeat Plaintiffs' counsel's strategies – regarding class certification, oppositions to motions to dismiss/dispositive motions, and settlement negotiations – before they happen to help achieve the best possible results for his clients.

About EPAY Systems

EPAY Systems provides cloud-based human capital management solutions that help businesses optimize their workforce, reduce labor costs, and ensure labor law compliance. Our time and labor management system, unified with our applicant tracking, HR, benefits administration, and payroll modules lowers labor costs by five percent or more for employers with an hourly workforce. EPAY's solutions are accompanied by administrative services, cutting-edge biometric time clocks and mobile app time tracking devices, and actionable analytics that help streamline your operations and reduce your labor spend.

Headquartered in Chicago, IL, EPAY Systems delivers HR solutions to over 75,000 worksites across the globe. For more information, visit www.EPAYsystems.com or call 877-800-3729.

Disclaimer

The contents of this document should not be construed as legal advice or a legal opinion on any specific facts or circumstances.

These materials are intended for general information purposes only, and you are urged to consult a lawyer concerning your own situation and any specific legal questions you may have.

Introduction

As biometric technology has become more advanced and affordable, more companies and employers have begun implementing procedures and systems that rely on biometric data.

"Biometrics" are measurements of individual biological patterns or characteristics such as fingerprints, voiceprints, and eye scans that can be used to quickly and easily identify consumers and employees. However, unlike social security numbers or other personal identifiers, biometrics are biologically unique and, generally speaking, immutable.

Thus, unlike a bank account or a social security number, which can be changed if it is stolen, biometric data, when compromised, cannot be changed or replaced, leaving an affected individual without recourse and at a heightened risk for identity theft.

Given the serious repercussions of compromised biometric data, a number of states have proposed or passed laws regulating the collection and storage of biometric data. Plaintiffs' attorneys are taking notice, as the number of class action lawsuits in this area has surged in recent months. Claims brought by plaintiffs for violation of the biometric privacy statutes are still largely untested, as these suits are still in the early stages of litigation.

Currently, there are three states that have statutes regulating the collection and storage of biometric data: Illinois, Texas, and Washington.[1] Of these three states, only Illinois provides a private cause of action enabling consumers and employees to seek damages on behalf of themselves and others similarly situated. The Washington and Texas biometric privacy laws only enable the state attorney general to enforce the respective statutes.

For this reason, this Guide focuses on the Illinois Biometric Privacy Act (BIPA) as the most restrictive biometric statute nationwide. To the extent that there are notable differences between the three statutes, such differences are also noted in this Guide.

---

1 Several other states (including Alaska, Massachusetts, Montana, and New Hampshire) have introduced similar legislation with varying levels of success. However, even in states where there is no law governing the collection and storage of biometric data exists, companies and employers should still take caution when collecting and storing biometric data because the practice could lead to invasion of privacy or negligence claims.

Understanding the Illinois Biometric Privacy Act

Overview of the BIPA

Illinois is the first state to enact a statute to regulate businesses' use of biometric identifiers/information ("BII"). The legislative history surrounding the bill suggests that the statute was implemented to protect consumers. Specifically, the Illinois legislature was moved by the fact that, unlike other types of personal identifiers that may fall into the wrong hands (e.g., Social Security numbers), BII cannot be changed. 740 ILCS § 14/5. The legislature was also motivated by the bankruptcy of Pay by Touch, the largest fingerprint scan system in Illinois, which left consumers unaware that their BII was being sold without assurances that the buyer would adequately protect their BII. The BIPA is still relatively new and therefore, courts are still interpreting the BIPA and other biometric laws in various ways and this area of law will continue to develop.

The BIPA regulates the "collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information." 740 ILCS 14/5(g). The BIPA defines a "biometric identifier" to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10.

"Biometric information," in turn, includes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual," but excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id*.

Notably, the definition of "biometric information" is very broad and, while the law is still unsettled, the statute arguably still applies if a company or employer converts an individual's biometric identifier into a mathematical code or other template and retains only the code or template and not the underlying biometric data.[2] As recently noted by the court in *Rivera v. Google, Inc*.:

> *The affirmative definition of "biometric information" does important work for the Privacy Act; without it, private entities could evade (or at least arguably could evade) the Act's restrictions by converting a person's biometric identifier into some other piece of information, like a mathematical representation or, even simpler, a unique number assigned to a person's biometric identifier. So whatever a private entity does in manipulating a biometric identifier into a piece of information, the resulting information is still covered by the Privacy Act if that information can be used to identify the person.*

Rivera v. Google, Inc., 238 F. Supp. 3d 1088, 1095 (N.D. Ill. Feb. 27, 2017) (refusing to dismiss a putative class action alleging that the cloud-based Google Photos service violated the BIPA by automatically uploading plaintiffs' mobile photos and

[2] The Washington law places restrictions on the "enrollment" of biometric identifiers, which is defined as "capturing" a biometric identifier or "convert[ing] it into a reference template." By contrast, the Texas law only protects biometric identifiers and does not contain a broader "biometric information" provision.

allegedly scanning them to create unique face templates for subsequent photo-tagging without consent).

Requirements of the BIPA

Notice and Consent

The BIPA prohibits companies from collecting employees' biometric information until the company notifies the employee in writing that the information is being collected. Specifically, the written notice must inform the individual of the "specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored and used." 740 ILCS § 14/15(b). Likewise, a company must obtain a written release from the individual enabling it to collect and store the information.

The Washington and Texas laws also require consent, but unlike the BIPA, do not specify that consent must be obtained in writing. The Washington law also contains an exception that other laws do not – that the law's notice and consent provisions do not apply to biometric data collected and stored by an employer for "security purposes," which is defined in the statute as biometric data that is stored for "the purpose of preventing shoplifting, fraud, or any other misappropriation or theft of a thing of value."

Written Policy

The BIPA also requires companies to develop a written policy establishing a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting them has been satisfied or within three years of the employee's last interaction with the employer, whichever occurs first. 740 ILCS § 14/15(a). The policy must be made available to the public. *Id*.

The BIPA has the most stringent retention requirements in that it states the information must be destroyed when the purpose for obtaining such data has been satisfied or within three years of the individual's last interaction with the employer, whichever occurs first. The Texas law requires only that employers destroy biometric data "within a reasonable time," but not later than one year after the biometric data is no longer needed. In Texas, if biometric data was collected for "security purposes," the purpose for collecting the data is presumed to expire on termination of the employment relationship. Finally, Washington's law requires employers to retain biometric data "no longer than is reasonably necessary" to comply with certain legal requirements and to provide the services for which the biometric data was collected.

Disclosure to Third Parties

In addition, a company may not disclose biometric information to a third party unless: it obtains consent for disclosure from the individual; the disclosure completes a financial transaction requested by the individual; the disclosure is required by

law; or the disclosure is required by a valid warrant or subpoena. 740 ILCS § 14/15(d).

Standard of Care

Also, the BIPA requires that a company use "the reasonable standard of care" within its industry for storing, transmitting and protecting biometric information and act "in a manner that is the same as or more protective than the manner in which the [company] stores, transmits and protects other confidential and sensitive information." *Id*. § 14/15(e).

The Texas law similarly requires employers to store, transmit, and protect the data from disclosure using reasonable care and in the same way the company treats other confidential information. Washington's law requires employers to take reasonable care to guard against unauthorized access to and acquisition of biometric data.

Statutory Damages

Under the BIPA, a plaintiff may sue a private entity for statutory violations in state court or as a supplemental claim in federal court. 740 ILCS § 14/20.

- The law authorizes a prevailing party to recover liquidated damages of $1,000 or actual damages, whichever is greater, for negligent violations of the Act. 740 ILCS § 14/20(1).
- The law authorizes a prevailing party to recover liquidated damages of $5,000 or actual damages, whichever is greater, for intentional or reckless violations of the Act. 740 ILCS § 14/20(3).
- The BIPA also authorizes recovery of an injunction for a prevailing party as well as reasonable attorneys' fees and costs. 740 ILCS § 14/20(3)-(4).

There is still uncertainty surrounding whether breach of all of the requirements of the BIPA constitute an independent "violation" of the BIPA for purposes of assessing statutory damages. Unsurprisingly, however, Plaintiffs in BIPA class actions to date have taken the position that each individual "scan" of biometric information (e.g., facial recognition, fingerprints, etc.) constitutes a separate violation entitling consumers and employees to statutory damages.

Best Practices for Compliance

Below is a list of best practices to be utilized by companies and employers utilizing biometric technology.

Provide Notice and Obtain Consent

Companies and employers utilizing biometric technology should provide notice (in writing) and obtain consent from individuals (also in writing) prior to capturing an individual's biometric data. *See Exhibit A: Sample Employee Notice and Consent Form.*

Have a Written Policy and Distribute to Individuals/Employees Along with Consent Form

The BIPA requires a business in possession of biometric data to have a publicly available, written policy stating the business's retention schedule for the data and rules governing its destruction.

Companies and employers utilizing biometric technology must develop such a policy and make it publicly available. As a matter of best practices, distribute this policy to individuals/employees prior to capturing an individual's biometric data. *See Exhibit B: Sample Biometric Privacy Policy for Employers.*

Ensure That Biometric Data Is Not Sold or Disclosed

Companies should ensure that neither the company nor any vendor storing biometric data on the company's behalf sells or discloses the data in violation of these laws and also not use the biometric data for any purpose outside of which consent was obtained.

The laws contain exceptions to this prohibition on disclosure where the individual consents to the disclosure, the disclosure completes a financial transaction requested by the individual, or the disclosure is permitted by law, order or warrant.

Again, outside of Texas, Washington, and Illinois, reasonableness would dictate that an employer should not disclose an employee's biometric data to others without consent under an invasion of privacy or negligence analysis.

For information regarding EPAY Systems' policies regarding data privacy (including biometric data) see *Exhibit C: EPAY Systems' Data Privacy Statement.*

Establish Protocols for Protecting Biometric Data

Companies and employers should protect biometric data in the same manner as they do with other confidential and sensitive information in their possession. Protocols for protecting biometric data can be covered in general information security policy or in a specific biometric data policy. *See Exhibits D: EPAY Systems' Data Security Protocol as well as Exhibit B.*

Ensure Compliance with Applicable Data Breach Notification Statutes If Biometric Data Is Compromised

Biometric data is considered "personal information" under a number of state data breach notification laws, including Illinois, Iowa, Nebraska, New Mexico, North Carolina, Wisconsin and Wyoming. Companies and employers storing biometric data (and vendors) must follow the requirements of these laws with regard to informing affected individuals of breaches/suspected breaches.

Understanding EPAY Systems' Biometric Technology

How EPAY's Biometric Technology Works

EPAY Systems' WalTer™ biometric time clocks utilize best in class technology for capturing biometric data, which is utilized and audited by the U.S. Department of Defence. Minutia points of an employee's finger are scanned and stored as a set of binary-encrypted mathematical scores (i.e. a biometric template), not a fingerprint image. The biometric data can only be decrypted by EPAY Systems' WalTer algorithm, which further eliminates the possibility of reverse engineering, or of an individual's biometric identifier becoming compromised.

When an employee clocks in or out for work, the system matches the newly-input minutia to the securely-saved minutia data. When there is a match, the employee is clocked in with an approval and the newly-input minutia is immediately destroyed.

EPAY's facial recognition technology works similarly to its Biometric finger minutia technology, except it uses facial minutia points instead of finger minutia points to determine a mathematical score.

Clients Can Provide/Collect Employee Notice and Consent Forms from Most WalTer Time Clocks

Requiring employees to sign a written consent form is always recommended. However, if your legal counsel approves, collecting consent forms on the WalTer time clocks is an option to provide notice and obtain consent.

EPAY clients can elect to present employees with Employee Notice and Consent Forms and obtain their electronic signature directly from WalTer T6, T11 and T16 time clocks. This is done by enabling the system's configurable Dynamic Attestation feature. To enable this feature, contact EPAY Support at 877-800-3729, option 2.

Once the Dynamic Attestation feature is enabled, the form is presented electronically to employees the next time they punch in or out, directly after they've completed their punch. After an employee completes the form, it is not presented to him/her again.

Exhibit A

Sample Employee Notice and Consent Form

BIOMETRIC TIME CLOCK - ASSOCIATE CONSENT FORM

I understand that _____ ("the Company") has engaged (EPAY Systems) to administer its biometric timekeeping system. EPAY Systems utilizes biometric technology for the purpose of identifying associates and recording time entries using a biometric time clock. I understand that biometric time clocks are generally computer-based systems that first capture some form of biometric identifiers. The computer system then extracts unique characteristic points known as "minutia" from my fingerprint image or facial scan and formulates a biometric template (i.e. a mathematical representation of the fingerprint scan or facial scan) used to verify an associate's identity. EPAY Systems system does not store images of associates' fingerprint scans. When an employee clocks in or out for work, the system matches the newly-input minutia to the securely-saved biometric template. When there is a match, the employee is clocked in with an approval and the newly-input minutia is immediately destroyed.

I acknowledge that I have received the attached Biometric Information Privacy Policy.

I consent, as a condition of continued employment, to providing biometric information for the purpose of identification and recording time entries when utilizing the Blueforce Time and Labor Management System.

_____

Associate Signature Date

_____

Associate Name (print)

Prueba Documental A

Notificación para Empleados y Formulario de Consentimiento de Muestra

RELOJ REGISTRADOR BIOMÉTRICO – FORMULARIO DE CONSENTIMIENTO DE ASOCIADO

Entiendo que _____ ("la Compañía") ha contratado a (EPAY System) para la administración de su sistema biométrico de cronometraje. EPAY Systems utiliza tecnología biométrica con el propósito de identificar a los asociados y efectuar un registro del tiempo con un reloj registrador biométrico. Entiendo que estos relojes registradores son, por lo general, sistemas computarizados que, en primer lugar, capturan cierta forma de identificadores biométricos. Luego, el sistema computarizado extrae unos puntos característicos únicos conocidos como "minucias", tomados de la imagen de mis huellas digitales o de un escaneo facial y crea una plantilla biométrica (por ejemplo, una representación matemática de mi huella digital o imagen facial) que se utilizará para verificar la identidad del asociado. El sistema de EPAY Systems no guarda las imágenes de las huellas digitales del asociado. Cuando un empleado marca la hora de entrada o salida del trabajo, el sistema asocia las minucias recién ingresadas a la plantilla biométrica propiamente guardada. Cuando se logra la asociación, se marca la hora de entrada del empleado con una aprobación y las minucias recién ingresadas se eliminan.

Reconozco que he recibido la Política de Privacidad sobre Información Biométrica adjunta a este documento.

Acepto, como condición para continuar en el empleo, proveer la información biométrica con fines de identificación y registro del tiempo cuando utilice el Blueforce TLM (Time and Labor Management) System.

_____

Firma del Asociado Fecha

_____

Nombre del Asociado (en letra de imprenta

Exhibit B

Sample Biometric Privacy Policy for Employers

BIOMETRIC INFORMATION PRIVACY POLICY

In order to efficiently and securely track employees' time records, _____ ("the Company") utilizes a biometric timekeeping system (EPAY Systems' Blueforce Time and Labor Management System). In accordance with the Illinois Biometric Information Privacy Act, the Company has instituted the following policy:

Biometric Identifier defined: "Biometric identifier" means a retina or iris scan, fingerprint or voiceprint, or scan of hand or face geometry.

Biometric Information defined: "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual.

Biometric Identifier/Information Collection: The Company utilizes biometric technology for the purpose of identifying employees and recording time entries using the Blueforce Time and Labor Management system. As part of this system, the Company/Vendor collects and/or stores employees' biometric identifiers and biometric information.

Consent: In order to use the biometric timekeeping system, employees will be asked to sign a consent form authorizing the Company to collect/capture employees' biometric identifiers and biometric information. It is a condition of employment with the Company that employees sign the consent form.

Disclosure: The Company will not sell, lease, trade, or otherwise profit from an employee's biometric identifier or biometric information. Nor will it authorize its timekeeping vendor to engage in any such activity. Neither the Company nor its timekeeping vendor will disclose or disseminate an employee's biometric identifier or biometric information unless:

The employee or the employee's legally authorized representative provides consent to such disclosure;

The disclosure completes a financial transaction requested or authorized by the employee or the employee's legally authorized representative;

The disclosure is required by state or federal law, or municipal ordinance; or

The disclosure is required pursuant to a valid warrant or subpoena.

Storage: The Blueforce Time and Labor Management system extracts unique characteristic points known as "minutia" from fingerprint images or facial scans and

formulates a biometric template (i.e. a mathematical representation of the fingerprint scan or facial scan) used to verify an associate's identity. The processed biometric template is stored/registered in a database for later comparison during an authentication. The actual value stored in the database is binary encrypted data which can only be decrypted by EPAY Systems WalTer algorithm. EPAY Systems system does not store images of associates' fingerprint scans. When an employee clocks in or out for work, the system matches the newly-input minutia to the securely-saved biometric template. When there is a match, the employee is clocked in with an approval and the newly-input minutia is immediately destroyed.

Retention Schedule: An employee's biometric information (i.e. biometric template) will be retained only until the initial purpose for collecting or obtaining the biometric identifiers or information has been satisfied, or within 3 years of the employee's last interaction with the Company, whichever occurs first.

Prueba Documental B

Muestra de Política de Privacidad Biométrica para Empleadores

POLÍTICA DE PRIVACIDAD SOBRE INFORMACIÓN BIOMÉTRICA

Con la finalidad de supervisar los registros de tiempo de los empleados de forma eficiente y segura, _____ ("la Compañía") utiliza un sistema biométrico de cronometraje (el Blueforce TLM Systems de EPAY Systems). De conformidad con la Ley de Privacidad de la Información Biométrica de Illinois, la Compañía ha establecido la siguiente política:

Definición del identificador biométrico: el "identificador biométrico" consiste en el escaneado de iris o retina, huellas digitales o de voz, o el escaneado de la geometría de manos o facial.

Definición de la información biométrica: la "información biométrica" consiste en cualquier información, sin importar la manera en que se capte, convierta, guarde o comparta, basada en el identificador biométrico de la persona y que se utiliza para identificarla.

Identificador Biométrico/Recopilación de Información: la Compañía utiliza la tecnología biométrica con la finalidad de identificar a sus empleados y llevar un registro de su tiempo con el Blueforce TLM system. Como parte de este sistema, la Compañía/Proveedor recopila y/o guarda los identificadores biométricos y la información biométrica de los empleados.

Consentimiento: con la finalidad de utilizar el sistema biométrico de cronometraje, se pedirá a los empleados que firmen un formulario de consentimiento, en el cual se autoriza a la Compañía a recopilar información biométrica y captar los identificadores biométricos de los empleados. Es una condición para el empleo en la Compañía que sus empleados firmen el formulario de consentimiento.

Declaración: la Compañía no venderá, alquilará, comercializará ni se beneficiará de ninguna otra forma del identificador biométrico ni de la información biométrica del empleado. Tampoco autorizará a su proveedor de cronometraje a que lleve a cabo ninguna de estas actividades. Además, ni la Compañía ni su proveedor de cronometraje divulgará o difundirá el identificador biométrico o la información biométrica del empleado a menos que:

el empleado o su representante legal autorizado lo permita;

la divulgación forme parte de una transacción financiera solicitada o autorizada por el empleado o su representante legal autorizado;

se exija la divulgación por parte del Estado, la ley federal, ordenanza municipal o

se exija la divulgación conforme a una orden judicial válida o emplazamiento.

Almacenamiento: el Blueforce TLM system extrae puntos característicos únicos conocidos como "minucias", tomados de la imagen de huellas digitales o de un escaneo facial y crea una plantilla biométrica (por ejemplo, una representación matemática de la huella digital o imagen facial) que se utiliza para verificar la identidad del asociado. La plantilla biométrica procesada se guarda/registra en una base de datos, para una comparación posterior durante una autenticación. El verdadero valor guardado en la base de datos consiste en datos binarios encriptados que pueden descodificarse únicamente con el algoritmo Walter de EPAY Systems. El sistema de EPAY Systems no guarda las imágenes de las huellas digitales del asociado. Cuando un empleado marca la hora de entrada o salida del trabajo, el sistema asocia las minucias recién ingresadas a la plantilla biométrica propiamente guardada. Cuando se logra la asociación, se marca la hora de entrada del empleado con una aprobación y las minucias recién ingresadas se eliminan.

Calendario de Retención: la información biométrica del empleado (esto es, su plantilla biométrica) se retendrá solo hasta que se haya cumplido el propósito inicial de recopilación de información o en el lapso de 3 años de la última interacción del empleado con la Compañía, lo que ocurra primero.

Exhibit C

EPAY Systems Data Privacy Statement

EPAY Systems does not/will not share collected application data with any third parties.

This includes customer and employee data, biometric identifiers, biometric information, punch times and corresponding latitude/longitude coordinates, etc. Data ownership resides solely with our clients as outlined in the Blueforce Time and Labor Management Service Agreement.

Employee biometric data contained on WalTer biometric time clocks is removed immediately upon an employee's termination.

However, employee biometric data remains on EPAY servers. Upon request, EPAY will immediately remove all biometric data stored on EPAY servers for terminated employees when they are marked as inactive in the system. EPAY requires clients to complete a written request form to authorize EPAY to remove biometric data of terminated employees on EPAY servers.

Exhibit D

EPAY System's Data Security Protocol

EPAY has invested heavily in resources to ensure our data security and infrastructure protocols (including biometric data) exceed industry best practices. We are also compliant with all applicable state Data Breach Notification Statutes.

We currently hold FedRAMP Ready status, which means our cloud security protocols meet the rigorous requirements of the U.S. government.

These data security protocols include:

- Developing and following a detailed IT security policy. Clients may request a confidential copy of this document from EPAY.
- Hosting all client data on a private cloud. All hardware and SQL systems are owned and managed by EPAY.
- Locating our dedicated servers in PCI-compliant SAS 70 Type II SSAE 16 SOC Certified data centers that feature 24/7 security and monitoring.
- Encrypting all data, using https-secure protocols for all system transactions. This includes using the SSL 256-bit AES protocol for data in transit and FIPS140-2 AES 256 protocol for data at rest.
- Using only Tier 4 data center locations that guarantee 99.95% uptime.
- Using proactive, proprietary system monitoring solutions to ensure EPAY server, network and applications run optimally without interruption.
- Biometric Security - Processed biometric templates (i.e. a mathematical representation of the fingerprint scan or facial scan) are stored/registered in a database for later comparison during an authentication. When an employee clocks in or out for work, the system matches the newly-input minutia to the securely-saved biometric template. When there is a match, the employee is clocked in with an approval and the newly-input minutia is immediately destroyed. The actual value stored in the database is binary encrypted data which can only be decrypted by EPAY Systems' Walter algorithm.