certiphi screening

white paper

ELECTRONIC SIGNATURES

National and global analysis

ELECTRONIC SIGNATURES:

HARNESSING NEW HIRING EFFICIENCIES WITH ELECTRONIC SIGNATURES

PURPOSE

This white paper provides detail on the use of electronic signatures ("e-signatures") from a national and global perspective. The introduction of e-signatures effectively renders electronic signatures as an acceptable form of written authorization for background checks conducted for employment-related purposes.

This paper will further outline electronic signature integration into a Web-based employment application management system, highlighting the improved efficiencies in authorizing and ordering background checks.

E-SIGNATURE GENERALLY

An e-signature refers to any electronic process used to indicate acceptance of a form or agreement. These methods range from email, phone, or other personal authentication processes. An e-signature may also include a specific type of signature referred to as a "digital signature." Digital signatures require the signer to authenticate their identity with a digital ID certificate.

While e-signatures are generally binding in every country, each jurisdiction has its own electronic signature law. There are three different types of e-signatures laws, which include: *Minimalist/ Permissive laws; Two Tier Laws; and Prescriptive laws*.

Minimalist/ Permissive

These laws permit e-signatures for all uses and can be adopted on any type of technology. Under minimalist laws, all types of virtual signatures, whether electronic or digital, will be accepted. Several regions implement minimalist e-signature laws such as the United States,[1] Australia,[2] New Zealand,[3] Thailand,[4] and Canada.[5] The United States "ESIGN" Act will be discussed in more detail below.

Two Tier

This is a hybrid approach where, similar to minimalist laws, most e-signatures from any type of technology will be accepted. However, two tier laws also provide for a class of approved technologies that may be used. Although approved technologies are available, most

1 ESIGN, 15 U.S.C. § 7001
2 Electronic Transactions Act of 1999
3 Electronic Transactions Act of 2002
4 Electronic Transactions Act B.E. 2544 (2001) (ETA)
5 Personal Information Protection and Electronic Documents Act SC 2000

030321

countries that implement two tier laws will allow private parties to agree to the acceptable form of signature. The European Union is an example where there is a clear preference for digital signatures over general electronic signatures. Regions that implement two tiered laws include countries within the European Union, China,[6] and Japan.[7]

Prescriptive Laws

This is the final type of e-signature law and is rarely adopted. Prescriptive laws are very strict and will only accept e-signatures made through a specific, limited type of technology. Additionally, only certain types of signatures will be accepted. The few jurisdictions that implement prescriptive laws include: Brazil,[8] Indonesia,[9] Israel,[10] Peru,[11] Philippines,[12] Russia,[13] Turkey,[14] and Uruguay.[15]

WHAT IS THE ESIGN ACT?

The Electronic Signatures in Global and National Commerce (ESIGN) Act is the e-signature law implemented in the United States. The ESIGN Act was designed to further the growth of electronic commerce in the United States; the Act provides electronic signatures with the same legal force as handwritten signatures on paper contracts.

The ESIGN Act is actually the third wave in a flurry of electronic commerce legislation that occurred in the 1990s and early 2000s. The first wave came from individual states, which only supported a specific type of electronic signature for a specific transaction.[16] The second wave of legislative activity was initiated by the National Conference of Commissioners on Uniform State Laws, who suggested a standard set of rules for electronic signatures that could serve in every state. The uniform set of rules was referred to as the Uniform Electronic Transactions Act (UETA), in 1999.[17]

In 2000, the ESIGN Act was signed into law, granting a nationwide legality to electronic contracts and electronic signatures. Although this law now exists, consumers still enjoy the freedom to choose between paper and electronic contracts. ESIGN broadly defines an electronic signature as an electronic "sound, symbol, or other process" that is executed by a person "with the intent to sign a record."[18]

6 Electronic Signature Law of the People's Republic of China
7 Law Concerning Electronic Signatures and Certification Services
8 Provisional Measure 2200-2
9 Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions
10 Electronic Signature Law 5761-2001
11 Digital Certificates and Signatures Law, La No. 27269
12 Republic Act No. 8792
13 Federal Law No. 63-FZ; Federal Law No. 149- FZ
14 Electronic Signature Law No. 5070
15 Law No. 18.600 on Electronic Documents and Electronic Signatures
16 Examples include Utah's Digital Signature Act of 1995, followed by legislation in California in 1995, and then in Illinois in 1998.
17 The Act validated electronic record and signatures and is adopted by several states.
18 ESIGN, 15 U.S.C. § 7006(5) "The term 'electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

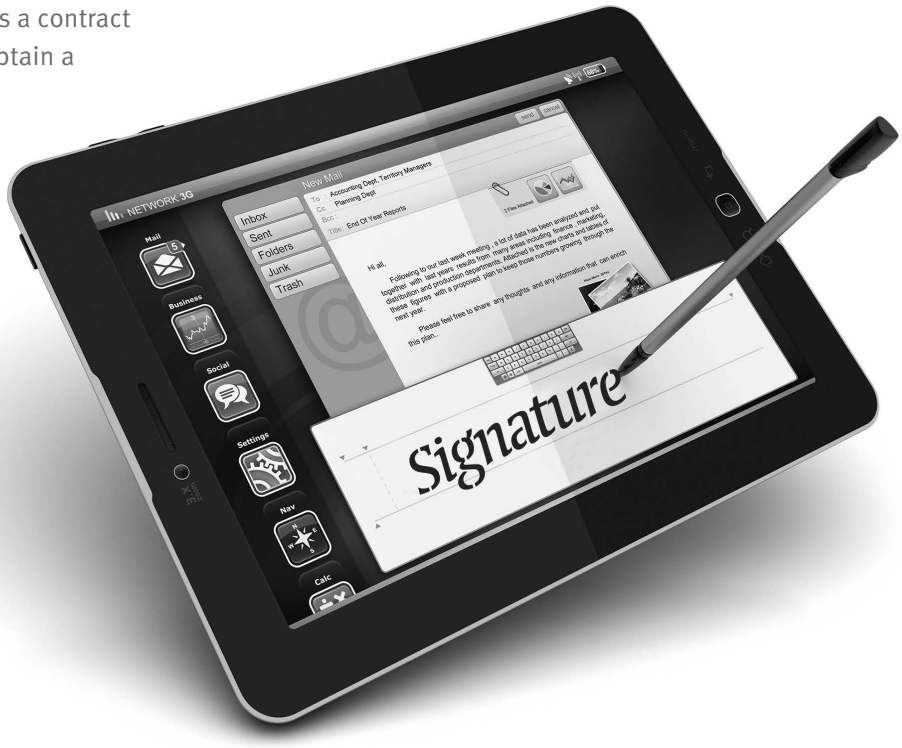
ESIGN and the FCRA

The 2001 FTC ESIGN ruling holds particular significance for employers who conduct background checks as part of the hiring process. In response to an inquiry, the FTC confirmed that under the ESIGN Act, an electronic signature satisfies the Fair Credit Reporting Act (FCRA)'s requirement to obtain the consumer's "written instructions" in order for a consumer reporting agency (CRA) to provide a consumer report for employment-related and other purposes.[19] In other words, an applicant or existing employee's authorization to conduct a background check may be legally given via e-mail, mouse click, or other electronic means.

The FTC established that text within the FCRA and the ESIGN Act establishes the legality of electronic signatures and contracts "with respect to any transaction."[20] The term "transaction" is defined in the ESIGN Act as "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons …" for the sale or exchange of personal property, goods, or services.[21] In the FTC's interpretation, this broad definition of "transaction" includes a contract or form that provides clear authorization to obtain a background check.

Furthermore, the ESIGN Act specifies that if, like the FCRA, a statute requires a contract relating to a transaction to be in writing, the electronic record of it must be in a form which can be retained and reproduced.[22] The FTC concluded that the consumer's electronic authorization for the background check would be valid as the FCRA's definition of "written instructions" as long as the stipulations for retention and reproduction were met.

The FTC's ruling on electronic signatures is limited to the authorization of background checks for employment purposes. The language of the ESIGN Act *implies* that an electronic signature could legally be used with other records involved in the hiring process, such as certifying the accuracy of an application. However, since a specific ruling on this usage has not been issued by the FTC, the legality of it is ultimately up to the courts to decide. HR professionals considering the usage of electronic signatures elsewhere in an employment application should consult with their legal departments.



19 See FCRA, 15 U.S.C. § 1681b(a)(2)
20 ESIGN, 15 U.S.C. § 7001(a)(1)& (2)
21 ESIGN, 15 U.S.C. § 7006(13)
22 ESIGN, 15 U.S.C. § 7001(e)

GLOBAL E-SIGNATURE LAWS

As specified above, there are three different types of e-signature laws that may be implemented. Below are charts that provide details on the e-signature laws available:

COUNTRY	E-SIGNATURE LAWS
Countries With *Permissive/Minimalist* Electronic Signature Laws	
Australia	(Electronic Transactions Act of 1999) Australia's Electronic Transactions Act is similar to the U.S. UETA (1999) and ESIGN Act (2000). It recognizes any virtual signature as legal and enforceable when a signature is required. Electronic signatures and digital signatures are synonymous in terms of their legality. Australia does not permit virtual signatures for documents related to migration or citizenship.
Canada	(Personal Information Protection and Electronic Documents Act, SC 2000, c5) Canada, like Australia and the U.S., allow for both electronic signatures and digital signatures to fulfil a signature requirement. As long as both signing parties consent to conduct business electronically, virtual signatures are considered valid unless a party can prove otherwise. Some *minor* nuances exist in the electronic signature law among the provinces.
New Zealand	(Contract and Commercial Law Act 2017(CCLA)) All parties may freely agree to conduct business electronically. While all virtual signatures are considered equal, all signing parties must agree on the type that will used. New Zealand does not explicitly prohibit virtual signatures for any type of transaction.
Thailand	(Electronic Transactions Act B.E. 2544 (2001) (ETA)) In Thailand, a virtual signature is referred to as a "data message," which is held as equally valid to that of a hand-written signature. All "data messages" are presumed to be valid unless proven otherwise. Thailand does not explicitly prohibit any documents from being signed via an electronic or digital signature.
United States	(Electronic Signatures in Global and National Commerce (ESIGN) Act of 2000) Thanks to the UETA and ESIGN Act, electronic signatures and digital signatures are considered equal, valid, and 100% legal in the eyes of the reigning electronic signature law. All parties must consent to conducting business electronically. The U.S. does not permit virtual signatures for some legally required notices to consumers.

COUNTRY	E-SIGNATURE LAWS
Countries With *Tiered* Electronic Signature Laws	
Argentina	(Digital Signature Law 25, 506) Argentina law subscribes to the tiered method of legalizing virtual signatures we described above. Additionally, the laws pertinent to virtual signatures in Argentina are parallel to UNCITRAL model law. Under Argentina's tiered infrastructure, electronic signatures are considered legal and enforceable, but digital signatures (a.k.a. qualified, certified, or advanced signatures) are considered to have greater evidentiary weight. Civil Code, Section 1197 binds all parties to an agreement after they consent to conducting business electronically.
Bermuda	(Electronic Transactions Act of 1999) Bermuda law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. Electronic signatures are automatically considered valid unless proof to the contrary is presented.
Chile	(Law 19.799) (Decree 181) Chile law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. Electronic signatures are automatically considered valid unless proof to the contrary is presented. Chile does not permit virtual signatures for matters related to acts and contracts where the law requires attendance of one or more of the parties.
China	(Electronic Signature Law of the People's Republic of China) Regulations pertinent to electronic signature law in China model a combination of EU's directive, UNCITRAL model law, and the United Nations Convention on Electronic Communications in International Contracts. Law subscribes to a tiered method of legalizing virtual signature, permitting both electronic and digital signatures. While electronic signatures are presumed valid unless proven otherwise, some judges have hesitated to honor their validity as the law demands. For this reason, it may be advisable to obtain longhand signatures for extremely sensitive documents.
Colombia	(Law 527 of 1999) (Law 962 of 2005-Electronic Invoice) (Law 964 of 2005- Electronic Securities) (Law 1150 of 2007- Public Procurement) Colombia's laws regarding virtual signatures are not clear cut. While technically a tiered model, court rulings have been somewhat ambiguous on defining the difference between electronic and digital signatures. Nevertheless, while a distinction between the two is not explicit, a Colombian Supreme Court decision on December 16, 2010 removed any doubt of electronic or digital signatures being recognized as valid, enforceable and legal signatures.

COUNTRY	E-SIGNATURE LAWS
Countries With *Tiered* Electronic Signature Laws	
Ecuador	(Law on Electronic Commerce, Electronic signatures and Data Messages (2002)) A written signature is not necessarily required for a valid contract - contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document. The Law on Electronic Commerce, Electronic Signatures and Data Messages and the General Regulation to the Law on Electronic Commerce, Electronic Signatures and Data Messages specifically confirm that contracts cannot be denied enforceability merely because they are concluded electronically.
European Union Austria Belgium Bulgaria Croatia Cyprus Czech Republic Denmark Estonia Finland France Germany Greece Hungary Ireland Italy Latvia Lithuania Luxembourg Malta Netherlands Poland Portugal Romania Slovakia Slovenia Spain Sweden (UK listed separately below)	(Electronic Identification and Authentication Services Regulation (eIDAS)) The EU is very much a tiered jurisdiction. In fact, many of the modern tiered infrastructures model their regulation after that of their electronic signature law, eIDAS. The defining difference between the EU and other tiered jurisdictions is the existence of three definitive types of virtual signatures: • **Simple Electronic Signature** (a.k.a. basic electronic signature or electronic signature): Data in electronic form (signatures) which are attached to or logically associated with other electronic data (documents, agreements, etc.) and which serve as a method of authentication. Must signal the signer's intent to sign, be initiated by the signer, and appropriately associated with the document being signed. • **Advanced Electronic Signature:** Must meet the requirements of the Simple Electronic Signature in addition to being: (i) uniquely linked to the signer; (ii) capable of identifying a signer; (iii) created using eSignature creation data that the signer can, with a high level of confidence, use under his/her self-control; and (iv) enabled with detecting alterations to a document(s) after its completion. • **Qualified Electronic Signature:** Qualified Electronic Signatures (QES) are parallel to digital signatures. However, the qualified digital certificate must be issued by a vendor (certificate authority) that meets the requirements of the eIDAS and that is accredited and supervised by designated authorities in the EU. In the EU, all three types of virtual signature are considered legal and enforceable, although certain types of sensitive documents may require an advanced or qualified signature. Parties are free to choose the type of signature appropriate for the mode and sensitive nature of their business.

COUNTRY	E-SIGNATURE LAWS
Countries With *Tiered* Electronic Signature Laws	
Hong Kong	(Electronic Transactions Ordinance) Hong Kong law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures, and parallels UNCITRAL model law. In Hong Kong, all parties must consent to conducting business electronically. However, consent does not necessarily need to be explicit and may be inferred by a party's action of electronically or digitally signing a document(s).
India	(The Information Technology Act of 2000 / 2006 amendment / 2008 amendment) India law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. Consent to conducting business electronically is not necessarily required, but is recommended. Additional technical and legal requirements exist when using digital signatures. Section 10A provides that where an agreement is "expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.
Japan	(Law Concerning Electronic Signatures and Certification Services) Japan law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. eSignatures are legal and enforceable in Japan.
Malaysia	(Digital Signature Act 1997) (Electronic Commerce Act 2006) Malaysia law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures, and parallels UNCITRAL model law. While a court may request supporting evidence for electronic signatures falling below the standards of a "Qualified Electronic Signature" as defined in UNCITRAL, all virtual signatures are deemed permissible and legally binding in a court of law. Malaysia does not permit virtual signatures for the creation of negotiable instruments, and other sensitive documents.
Mexico	(Code of Commerce, Federal Civil Code, Federal Civil Code, Federal Code on Civil Procedures, and other laws contain amendments and provisions governing the use of virtual signatures) Mexico law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. Mexico does not prohibit virtual signatures for any type of document, but may require certification of official documents and tax related documents to be completed with a digital signature.

COUNTRY	E-SIGNATURE LAWS
Countries With *Tiered* Electronic Signature Laws	
Norway	(Electronic Signatures Act of 2001) Norway law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures.
Republic of Korea	(Digital Signature Act) The Republic of Korea subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. All parties must consent to conducting business electronically. Further, if the consent, signer's identity, or originality of the documents are questioned, then the validity of the signature must be determined by interpreting the party's intent to sign in correlation with the context of the document(s). The Republic of Korea does not explicitly prohibit any specific type of document from being completed with virtual signatures.
Saudi Arabia	(Electronic Transactions Law; Article 24 Amendment) Under Saudi law, a written signature is not necessarily required for a valid contract - contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document. Article 5 of the Electronic Transactions Law specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically.
Singapore	(Electronic Transactions Act of 2010) (Personal Data Protection Act of 2012) Singapore subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. Per Singapore law, the type of virtual signature used must either be "(1) as reliable as appropriate for the purpose for which the electronic record was generated or communicated, or (2) proven in fact to have identified the signatory and to indicate signatory's intention with respect to the information by itself or together with further evidence. Singapore does not permit virtual signatures for negotiable instruments.
South Africa	(Electronic Communications and Transactions Act of 2002, Act No. 25) South Africa subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures. All parties must consent to doing business electronically, but do not necessarily need to consent on the type of virtual signature used. No matter the type of virtual signature used, it must (1) identify the party and indicate their intent/approval and (2) be reliable and appropriate for the context and content of the document(s).

COUNTRY	E-SIGNATURE LAWS
Countries With *Tiered* Electronic Signature Laws	
Switzerland	(Swiss Federal Act on Electronic Signatures (FAES)) Switzerland law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures, and parallels UNCITRAL model law. Article 14 specifically states that electronic signatures may replace handwritten signatures. Switzerland does not explicitly prohibit any specific type of document from being completed with virtual signatures, but caution should be exercised for documents related to forms requiring notary, and other sensitive documents.
Taiwan	(Electronic Signatures Act 2001-11-14) Taiwan law subscribes to a tiered method of legalizing virtual signatures, permitting both electronic and digital signatures, and parallels UNCITRAL model law. Expressed consent is of particular importance in Taiwan. While Taiwan has not excluded any type of document from its laws governing virtual signatures, many government agencies have announced they will not accept documents that are electronically or digitally signed. **Note:** Some Taiwanese agencies have excepted themselves from the law.
United Kingdom	(The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No. 696)) (Electronic Communications Act of 2000, Section 7) While now separate from the EU, the U.K. has enacted electronic signature law nearly identical to eIDAS through its Electronic Identification and Trust Services for Electronic Transactions Regulation (2016 No. 696) and Section 7 of its Electronic Communications Act (2000).
Vietnam	(Decree No. 26/2007/ND-CP detailing the E-Transactions Law on Digital Signatures and Digital Signature Certificate Service (2007); Civil Code No. 91/2015/QH13 (2015)) Under Vietnamese law, a written signature is not necessarily required for a valid contract - contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document (Civil Code, Article 124). The Law on E-Transactions specifically confirms that contracts cannot be denied enforceability merely because they are concluded electronically (Law on E-Transactions, Article 14.1). To prove a valid contract, parties sometimes have to present evidence in court. Leading digital transaction management solutions can provide electronic records that may be admissible in evidence to support the existence, authenticity and valid acceptance of a contract (Law on E-Transactions, Article 14.2).

COUNTRY	E-SIGNATURE LAWS
Countries With *Prescriptive* Electronic Signature Laws	
Brazil	(Provisional Measure 2200-2) Brazil follows the UNCITRAL model law, but only legally recognizes virtual signatures that utilize the Brazilian Public Key Infrastructure (PKI). So long as the Brazilian PKI is used, all virtual signatures are considered legal and enforceable. Brazil does not explicitly prohibit any specific type of documents from being completed with a virtual signature.
Indonesia	(Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions) Indonesia law only recognizes digital signatures using a digital certificate provider that's registered with the country's Ministry of Communication and Information Technology. Further, the digital signature vendor must have all its data centers and disaster recovery centers located within Indonesia's borders.
Israel	(Electronic Signature Law 5761-2001) Israel law will only legally recognize a "certified signature" (digital signature). Israel follows a similar model to the EU apart from recognizing basic electronic signatures on documents which require a signature. Israel does not explicitly prohibit any specific type of documents from being completed with a digital signature.
Peru	(Digital Certificates and Signatures Law, Law No. 27269) Peru only legally recognizes digital signatures issued with a digital certificate and vendor that meets the law's specified minimum requirements. While Peru issues approved certification providers, it will legally recognize those outside its jurisdiction so long as it meets the same standards. Peru does not explicitly prohibit any specific type of documents from being completed with a digital signature.
Philippines	(Electronic Commerce Act of 2000 (Republic Act No. 8792)) Section 8 of the Act specifies that all signatures must use a digital certificate. Parties are free to agree between themselves that electronic signatures will be binding, the preference is for the use of digital signatures with certificate.
Russia	(Federal Law No. 63-FZ "On Demand Signature (July 1, 2011) (Federal Law No. 149-FZ "On Information, Information Technology and Protection of Information" (July 27, 2006)) (Part Four of Civil Code of the Russian Federation (Art. 160)) In Russia, all parties must consent to doing business electronically. Only digital signatures are recognized as legal and valid. Under Russian law, a digital certificate and signature vendor must be certified by the Russian government (despite courts often upholding basic electronic signatures as enforceable). Russia does not explicitly prohibit any specific type of documents from being completed with a digital signature.

COUNTRY	E-SIGNATURE LAWS
Countries With *Prescriptive* Electronic Signature Laws	
Turkey	(Electronic Signature Law (No. 5070)) Turkey mirrors the UNCITRAL Model law. Basic electronic signatures are not addressed by Turkey law. Digital signatures are recognized as legal and valid so long as the digital certificate is issued by a qualified services provider. Should a party challenge the validity of a digital signature, that party is burdened with proving it is invalid or forged. Turkey does not explicitly prohibit any specific type of documents from being completed with a digital signature.
Uruguay	(Law No. 18.600 on Electronic Documents and Electronic Signatures) The law allows the parties to agree privately to the form of signature, but the consent can be challenged by either party at a later date. Electronic signatures are nevertheless used commonly in Uruguay.

WEB INTEGRATION PROCESSES

This section provides an overview of e-signature integration into a web-based employment application management system.

E-Signature Law Compliance

The electronic signature technology provided in Certiphi Screening's online employment application solution, ApplicationStation®, complies with e-signature law requirements. ApplicationStation® is a background screening tool that provides employers with a platform for employment applications. Controls are in place to ensure that once this information is submitted, it cannot be changed. ApplicationStation® stores paper employment applications on a secure website that may only be accessed with an applicant's username, password, and a special code provided by the employer.

The "Disclosure and Authorization section" of the online application is where an electronic signature can be used to authorize a background check. At the bottom of the authorization form, there are fields where an applicant can enter his/her name, indicate agreement to the background check by clicking a box next to the word "Agree," and enter the date. Once a completed application is submitted, the applicant can view the document in Word format, and print out a copy for their records.

The ApplicationStation® system allows employers to securely receive, track, and view submitted applications and authorization forms via a private extranet. It also enables employers to immediately request background checks online. Once a request is submitted, the system automatically pulls the data necessary for the background check from the appropriate application. Applicant data collected through ApplicationStation® is stored in Extensible Markup Language (XML); as a result, the ApplicationStation® system can populate Equal Employment Opportunity (EEO) forms and reports, as well as I-9 Employment Eligibility Verification forms.

In conclusion, the FTC's clarification of the usage of electronic signatures to authorize background investigations allows employers to harness new levels of hiring efficiency. This is the case when either complying with the ESIGN Act or another global e-signature law. Online employment applications with integrated electronic signature technology allow for further integration of the employee screening process, saving time and reducing hiring costs.