HUMAN RESOURCES INFORMATION SYSTEMS: REVIEWING YOUR HRIS SYSTEM TO ENSURE IT CREATES ADMISSIBLE AND PERSUASIVE RECORDS

Gregory T. Casamento, Patrick J. Hatfield, and Hanna Norvell

Employers currently using or considering moving to an electronic Human Resources Information System (HRIS)[1] should review those systems to ensure that any notices, policies, training, evaluations, codes of conduct, disclosures and contracts, such as arbitration agreements or restrictive covenants,[2] generated by the HRIS and signed or acknowledged by employees electronically are as enforceable as those signed in wet ink on paper. Over the last few years, courts have explained the flaws to such systems when the enforceability of these agreements are challenged by employees.

To help employers mitigate the risks, human resources professionals can use a Six Point *e*-Risk Analysis Framework that analyzes the following six risks associated with an HRIS: (1) authentication risk, (2) repudiation risk, (3) admissibility risk, (4) compliance risk, (5) adoption risk, and (6) relative risk.[3] Through the use of the *e*-Risk Analysis Framework, employers first identify, then mitigate, the most common risks to the enforcement of their electronically signed agreements or other documents. Moreover, through the identification and mitigation process, most employers will conclude, as we have, that with an appropriately designed and implemented process, an employer can actually create electronically signed or acknowledged agreements that are as enforceable, if not more so, than those signed with wet ink on paper.[4]

To demonstrate how an employer can use the *e*-Risk Analysis Framework with its HRIS, this article first discusses the six risks that the Framework helps employers identify and then shows how employers can develop a process to mitigate those risks. The article then discusses four relevant HRIS court opinions[5] to show how the risks faced by each employer in those situations were

GREGORY T. CASAMENTO is a partner in the New York office of Locke Lord Bissell & Liddell LLP. Mr. Casamento's practice focuses on business, commercial, employment and intellectual property litigation. He has significant experience litigating restrictive covenant, breach of contract and the enforcement of arbitration agreements before both State and Federal Courts. As a member of Locke Lord's Technology Transactions group, Mr. Casamento regularly assists clients in review of e-process systems. He is also highly knowledgeable in e-Matters (e-signatures, e-discovery, e-admissibility), and regularly addresses a number of prestigious organizations and trade associations regarding the admissibility and enforceability of e-signatures, e-contracts, and e-records.

PATRICK J. HATFIELD is a Partner in the Corporate Department of the Atlanta office of Locke Lord Bissell & Liddell LLP and serves as co-chair of the firm's Technology Transactions Group. Mr. Hatfield's practice is highly focused on issues surrounding electronic signatures, outsourcing, and software licensing and development. Mr. Hatfield is a frequent and sought after speaker and regularly addresses some of the most highly regarded industry associations in the country on electronic signatures and a number of e-Matters related topics.

HANNA NORVELL is a partner in the Houston office of Locke Lord Bissell & Liddell LLP. She is Board Certified in Labor and Employment Law by the Texas Board of Legal Specialization, and her practice exclusively serves employers regarding any employment related issues, including compliance, counseling and litigation. She has successfully litigated the issue of an enforceable arbitration agreement signed electronically wherein the matter was compelled to arbitration.

or could have been mitigated by the *e*-Risk Analysis Framework.

SIX POINT *E*-RISK ANALYSIS FRAMEWORK

Authentication Risk

This is the risk that the person signing the agreement is in fact not the person he or she claims to be, also referred to as the "forger risk." To mitigate the Authentication Risk, employers should configure their HRIS to properly authenticate the identity of the person signing. Employers can authenticate employees on an HRIS through the use of secure log-in names, passwords, and pin numbers, information *created by and known only to* the individual employee. Default or other access by a supervisor or other person should be avoided. With new employee applicants, employers can use third-party databases to verify the applicant's identity. Employers should seek to record and archive this authentication process, often referred to as "capturing an audit trail," which the HRIS then securely archives for later secure retrieval if the employee claims he or she never signed something on the system. If the employer opts not to include the authentication process in the audit trail, then the employer may not have access to reliable evidence to establish the actual identity of the employee. Ideally, the employer calibrates the level of authentication with the employer's assessment of the authentication risk within their organization.

Repudiation Risk

This is the risk that the employee later repudiates the terms and conditions in the record bearing his or her signature. For example, the employee acknowledges that he or she signed the document attached to or logically associated with his or her signature, but claims that the document contains terms and conditions different than those in the original agreement because it was changed after it was signed or that what they signed did not sufficiently describe the terms or conditions at issue or that the employee otherwise did not receive some required notice.

HRIS often can be configured to reduce the repudiation risk far below such risk associated with paper documents signed in wet ink, especially multi-page documents or documents which refer to other documents. For example, HRIS can cryptographically seal each document upon the signing of that document by the employee, thereby rendering such document unalterable without detection. Documents electronically sealed in this fashion are likely to pass the admissibility threshold (see discussion below) and once such documents are admitted into evidence, employers are likely to have meaningful, persuasive evidence as to why such documents could not have been altered without detection and should therefore be enforced as written against the employee.

Admissibility Risk

This is the risk that a court refuses to admit into evidence copies of electronic documents generated, presented, signed, secured, archived and retrieved by the employer's HRIS because of evidentiary "authentication" issues, a condition to admissibility of any document. The rules of evidence regarding authentication, including the required evidentiary foundations, that apply to paper documents and wet ink signatures apply also to electronic documents signed electronically, stored electronically and retrieved electronically.[6] Thus, the Federal Rules of Evidence, or their state equivalents, will govern the admissibility of documents presented, signed, secured, archived and/or retrieved by an HRIS.[7]

Employers may use HRIS to create what are often referred to as "signing ceremonies." These are the processes by which employees sign documents in the HRIS, in ways to satisfy the admissibility standards in the Federal Rules of Evidence. Signing ceremonies are useful to prove at trial the authenticity of a document retrieved by HRIS because the ceremony can create a record of the entire signature ceremony process, including: (a) the terms and conditions presented to the employee with which the electronic signature will be logically associated; (b) the specific act of the employee expressing his or her intent to be bound to those terms and conditions, as called for in those same terms and conditions; and (c) the circumstances under which the employee's signature was obtained.[8] This information all goes to establish the authenticity of the document (containing the terms and conditions) stored in the HRIS. There will need to be one or more witnesses who can explain the process. Without the appropriate witness (from the HRIS vendor or the information technology department) to provide an affidavit or live testimony as to items (a) to (c) above, the evidence will not be admissible and therefore a court is likely to make a finding of no enforceable agreement.[9]

The standard for the authentication of evidence under the

Federal Rules of Evidence is contained in Rule 901, Requirement of Authentication or Identification, which provides that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[10] As stated throughout the relevant case law, "'reliability must be the watchword' in determining the admissibility of computer generated evidence."[11] The "factors [must] effectively address a witness's familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be acquainted with the technology involved in the computer program used to generate the evidence."[12]

Certain subparts of Sections 901 and 902 of the Federal Rules of Evidence are particularly suited to address the admission of electronic signatures and records signed using an HRIS: Sections 901(b)(1), (3), (4) and (9), and 902(7) and (11). Rules 901(b)(1), (3), (4) and (9) require witness testimony to authenticate proffered evidence, while 902(7) and (11) allow for self-authentication.[13] An HRIS need only be authenticated once through one of these methods, whichever is best applied to the situation at hand.

F.R.E. 901

A witness with direct knowledge, pursuant to F.R.E. 901(b)(1), or an expert witness with learned knowledge, pursuant to F.R.E. 901(b)(3), are certainly two fairly straightforward methods an employer could use to admit hard copies of documents signed using an HRIS. F.R.E. 901(b)(4), which permits exhibits to be authenticated by appearance, contents, substance, internal patterns, or other distinctive characteristics "is one of the most frequently used [rules] to authenticate [electronic signatures] and other electronic records."[14] F.R.E. 901(b)(9), which authorizes authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result," is "one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers" and is frequently used as a litmus test for admissibility of computer-related information.[15] "[It] dictates that the inquiry into the basic foundational admissibility requires sufficient evidence to authenticate both the accuracy of the image *and* the reliability of the machine producing the image."[16]

HRIS should use a process to secure each document after it is signed to allow employers to configure the HRIS to meet the admissibility standards under the subsections in F.R.E. 901. The testimony of a witness with knowledge of the specific transaction will satisfy F.R.E. 901(b)(1), and a learned expert witness should suffice under F.R.E. 901(b)(3). An expert witness knowledgeable about the contents, substance and distinctive characteristics of the HRIS and the process of creating, presenting, signing, securing, archiving and retrieving the documents in question should satisfy F.R.E. 901(b)(4), while expert testimony describing how the HRIS accomplishes the foregoing accurately should suffice under F.R.E. 901(b)(9).

In addition to the express language of F.R.E. 901(b)(9), Imwinkelried's *Evidentiary Foundations* provides a supplemental eleven-step process under the Rule for the admission of computer generated records.[17] Most of the testimony proffered under these eleven steps is a simple recitation of facts that HRIS should meet. More challenging is step four, which requires expert testimony that the "procedure has built-in safeguards to ensure accuracy and identify errors…regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging changes, backup practices, and audit procedures to assure the continuing integrity of the records."[18]

Expert witness testimony seeking the admission of signatures and documents from the HRIS pursuant to F.R.E. 901(b)(9) would include:

- The manner in which the HRIS server(s), as appropriate, are used to generate electronic signatures and documents;
- The reliability of these servers;
- Procedures for manual data entry and system controls; and
- Safeguards to ensure accuracy and identify errors (i.e., safeguards, access rules and other controls on the environment that govern the flow of information through its system), tamper resistant software, use of cryptographic technology, and that all of these meet or exceed industry standards.

Following initial court decisions recognizing the safeguards of a particular HRIS might reduce the risk for future challenges and result in stipulations to the authenticity of electronic signatures created by that and comparable systems, such that in the initial cases witness testimony is required but in future and subsequent cases it is not. Notwithstanding, from the outset, there will be ample evidence to lay the appropriate foundation for the admission of electronic signatures created by the HRIS, assuming risks are adequately managed and appropriate witness testimony can be obtained.

F.R.E. 902

Although in a major dispute testimony may be necessary regarding the HRIS and the authenticity of its process, as noted above, documents presented, signed, secured, archived and retrieved using the HRIS may also be admitted as self-authenticating documents under F.R.E. 902(7). Judge Grimm, in the extremely thorough opinion in *Lorraine v. Markel*, stated that: "[e]xtrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:…(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin."[19] "Under Rule 902(7), labels or tags affixed in the course of business require no authentication. The HRIS will collect and record information showing the entire signature ceremony. The identification markers alone stored in the secure container may be sufficient to authenticate an *electronic record* and *electronic signature* under Rule 902(7)."[20]

F.R.E. 902(11) of the Federal Rules of Evidence might also be considered for authentication of documents presented, signed, secured, archived and retrieved using electronic signatures and records generated by an HRIS. As Judge Grimm noted: "Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial."[21] The primary reason one would seek to authenticate electronic evidence using this rule is that it permits a written declaration by a custodian rather than oral testimony, which under most circumstances makes it preferable to F.R.E. 901(b)(4) or (b)(9). F.R.E. 902(11) addresses:

> Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record—
>
> (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
>
> (B) was kept in the course of the regularly conducted activity; and
>
> (C) was made by the regularly conducted activity as a regular practice.[22]

Rule 902(11) was designed to work in tandem with an amendment to Rule 803(6) to allow proponents of business records to qualify them for admittance with an affidavit or similar written statement rather than the live testimony of a qualified witness. In addition to the affidavit requirements, there is a notice requirement to afford opposing parties an opportunity to review the document and affidavit to challenge its authenticity.[23] Thus, assuming no challenge, F.R.E. 902(11) is one of the best ways to secure the admission into evidence of signatures and documents executed using an HRIS.

As explained above, critical in the admissibility analysis and the overall enforceability of documents executed using an HRIS is the requirement of a secure method to archive and retrieve the documents so they cannot be altered after signature. The HRIS should also use a form of e-vaulting, such that the HRIS can securely archive signed documents to show the documents were not altered after signature, and secure retrieval capabilities. Assuming these guidelines are followed, the HRIS should produce admissible agreements.

Compliance Risk

The Compliance Risk is defined as the risk that the HRIS fails to comply with legal and regulatory requirements. This might result in employees being able to void electronically signed agreements.[24] Employers must be aware that their HRIS may need to be configured to meet certain legal and regulatory requirements, depending on states where the agreements are signed, industry, or other issues. This might require that each agreement presented and/or signed by the employee is presented in such a way, i.e., content, sequence, and disclosure, so that no regulatory objection can be made to enforcement. Users may configure HRIS to reduce the compliance risk associated with the transactions below the risk associated with similar transactions using wet ink and paper by designing the HRIS so that all regulatory disclosures are made before an employee can sign, through use of the audit trail, and setting up auto notifications when certain compliance issues arise.

Adoption Risk

This is the risk that employees will fail to adopt the HRIS because it is too burdensome, complicated, or otherwise non-employee friendly. Companies should be able to reduce the adoption risk by beta testing their HRIS with a select group of employees to work out any adoption type issues. Employers should also offer employees various types of incentives to encourage HRIS use, such as making employee pay and benefits information available on the HRIS, requiring employees to use HRIS for vacation or other personnel requests, or even providing other incentives to get employees to use the system. Moreover, the HRIS should be designed so that the system tracks and, when necessary, will send alerts to HR, management or other designated parties, if employees fail to adopt and therefore do not sign agreements or review notices presented through the system. Such efforts should mitigate against the adoption risk.

Relative Risk

It is important for employers to consider the risks of a given HRIS in the context of the risks associated with a paper and wet ink process. Considering the risks of the electronic signature process relative to the corresponding risks associated with the paper and wet ink signature process allows users to better assess the risks inherent in the electronic process, versus risks that are inherent in every process.

Our view is that HRIS is capable of being configured to reduce the risks considerably *below the corresponding risks of using paper and wet ink*. For example, an HRIS can be configured to prevent an agreement from being signed by the employee if there are any blanks in the document to be signed, prevent any document from being submitted by the employee unless all of the required steps, including execution of or acknowledgement of receipt of all disclosures, are fulfilled, prevent loss of all or portions of documents, and prevent employees from crossing out or modifying portions of documents or other issues common with hard copy agreements. Moreover, an HRIS can more easily track which employees have signed the necessary agreements and alert the necessary personnel to take actions regarding unsigned documents. Once signed, the HRIS secures the agreements from being altered without detection or lost. Employers may configure HRIS for various types of signature ceremonies for various types of employees. This configuration can calibrate the risk mitigation approaches discussed in this article, with the employer's concerns about the various risks for each category of employee. This can be done in such a way that the employer can, in all likelihood, configure HRIS so the electronic signature process has less risk than the paper and wet ink process.

In having identified the six risks that can be mitigated using the *e*-Risk Analysis Framework, we now move to a discussions of four cases that demonstrate how some of these risks have played out in employment disputes.

Campbell v. General Dynamics: Failure to Mitigate the Repudiation, Adoption, and Relative Risks Results in Unenforceable Arbitration Agreement

Campbell v. General Dynamics Government Systems Corporation[25] shows what can happen when a company fails to adequately consider the repudiation risks when implementing a new HRIS process. The decision also provides some interesting discussion points for employers looking to mitigate the adoption and relative risks.

In that case, General Dynamics failed to ensure that its HRIS gave Mr. Campbell, its employee, adequate notice of the changes in the terms of his employment, which allowed Campbell to repudiate his employer's arbitration policy of which he had received notice through email. Notwithstanding the Court's failure to enforce the arbitration agreement against Mr. Campbell, it did discuss several methods employers should consider in designing and implementing an HRIS to mitigate the risks identified by the *e*-Risk Analysis Framework.

General Dynamics sought to require all of its employees, as a condition of their continued employment, to resolve all future employment disputes or claims through binding arbitration. Instead of using its traditional method of sending employees such policy changes in hard copy that required the employees wet ink signature to acknowledge receipt of the change, General Dynamics notified all of its employees through a new email system. There was no dispute that Mr. Campbell received the e-mail, however, the actual arbitration policy and the revised employee handbook were not contained in the text of the e-mail. Instead, the email contained a hyperlink that, if accessed by Mr. Campbell, brought him to a Web site containing the policy. General Dynamics' system did not track whether Mr. Campbell accessed the Web site containing the policy.

Mr. Campbell brought suit in court seeking to recover damages for discrimination on the basis of a disability. General Dynamics responded with a motion to compel arbitration under the electronically sent arbitration policy. As reported in the District Court and First Circuit Court of Appeals decisions, Mr. Campbell argued that the policy did not apply to him because the General Dynamics' notification process, consisting of the email containing the hyperlink, did not provide him with sufficient notice of the policy change requiring all employees to arbitrate employer-employee disputes. Therefore, Mr. Campbell argued General Dynamics could not bind him to arbitration.

In separate opinions, both the District Court and then the First Circuit Court of Appeals sided with Mr. Campbell, finding that General Dynamics' e-mail process did not give Mr. Campbell sufficient notice of a change in policy necessary for the Court to hold that Mr. Campbell had waived his right to bring employment discrimination claims in court.

Both opinions discussed the various reasons General Dynamics' email provided insufficient notice to Mr. Campbell, each of which is instructive in highlighting one or more of the risks identified and mitigated by application of the *e*-Risk Analysis Framework.

In an example of how General Dynamics failed to mitigate the adoption risk, the court discussed how this was General Dynamics' first attempt at communicating a change to its employment policies to its employees through email instead of through its traditional method, e.g., by sending the employee an actual copy of the policy memorializing the significant change in writing, requiring the employee's "wet ink" signature, and then placing the signed writing in the employee's personnel folder. In failing to mitigate the risk, General Dynamics could not show that Mr. Campbell, a user of the paper and wet ink system, adopted (or used) the new HRIS.

General Dynamics also failed to mitigate the repudiation risk because it failed to have Mr. Campbell elicit a response or acknowledgment he had read the e-mail and the link to the new policy, such as requiring him to acknowledge receipt or to click a box on a computer screen indicating that he had read the policy. This allowed Mr. Campbell to repudiate the agreement, or in other words, argue that while he had received the email, he never saw the agreement.

General Dynamics failed to state in the substance of the e-mail that the new arbitration policy had contractual significance and that the policy contained an arbitration provision that would waive the employee's right to bring workplace disputes in court.

Based on General Dynamic's failures, the court held that, "a reasonable employee could read the e-mail announcement and conclude that the Policy presented an optional alternative to litigation rather than a mandatory replacement for it."[26] Notwithstanding the court's decision not to enforce the arbitration agreement against Mr. Campbell, the court did explicitly recognize, an "e-mail, properly couched, can be an appropriate medium for forming an arbitration agreement."[27]

The lesson of *General Dynamics* is simple: mitigate up front the risks in the design and implementation phase of an HRIS so that it clearly requires employee adoption, and provides clear and explicit notice to employees of the terms, conditions or changes in their employment, thereby preventing repudiation and allowing the employer to prove that its employees received notice of these terms, conditions or changes and should be bound.

Kerr v. Dillard: The HRIS's Failure to Mitigate the Authentication, Adoption and Relative Risk Led to the Court's Refusal to Enforce an Arbitration Agreement

The recent case of *Kerr v. Dillard* provides a good example of where an HRIS implementation failed to address the authentication, relative and adoption risks.[28] There, Dillard's[29] implemented an HRIS that required all of its store associates to electronically sign employment arbitration agreements through mydillards.com, Dillard's employee intranet system. Every Dillard's associates had a unique, confidential password, created by and known only to the associate.

Dillard's, however, also gave store supervisors the ability to log in to an associate's account by resetting the associate's confidential password and logging in under the associate's default password.

After an associate accessed mydillards.com, the system required the associate to execute the employee arbitration agreement by: (1) entering his or her social security number or associate identification number (AIN); (2) entering his or her secure password; and (3) clicking the "accept" option at the bottom of the arbitration agreement screen. The system would then generate an e-mail to the associate's Dillard's e-mail account, confirming that the associate had signed the arbitration agreement.

In an example of Dillard's failing to mitigate the adoption risk, for a period of five months Ms. Kerr refused her supervisors' repeated requests that she log on to her mydillards.com account to electronically sign her employee arbitration agreement. Ms. Kerr based her refusal on the misunderstanding that when she first became employed at Dillard's, she had not signed an employee arbitration agreement. Ms. Kerr believed that if she accessed the HRIS and electronically signed the employee arbitration agreement, she would give up some of her legal rights.

Five months after Dillard's first implemented the employee arbitration requirement on mydillards.com, Ms. Kerr had still not adopted the system. In fact, the evidence at trial showed Ms. Kerr had only accessed the system on three occasions: February 10, April 28, and August 24, 2006, with the April 28 access being the subject of the litigation. On the previous day, April 27, Ms. Kerr had missed work. When Ms. Kerr's supervisor asked Ms. Kerr why she had missed a scheduled day of work, Ms. Kerr attributed her absence to not knowing how to access her work schedule through mydillards.com. Ms. Kerr's supervisor then took Ms. Kerr to the Dillard's employee break room, where Dillard's had a computer kiosk for employee use, to show Ms. Kerr how to access her schedule on mydillards.com, and the supervisor actually accessed her account for her through the default password. The system recorded that at or near this time, Ms. Kerr signed her employment arbitration agreement and a confirmation e-mail was sent to Ms. Kerr's Dillard's e-mail account, which was opened. The system records also demonstrated that the e-mails on Ms. Kerr's intranet account were opened on only three previous occasions: February 10, April 28 and August 24, 2006.

Some time later, Dillard's terminated Ms. Kerr, and in response, she brought race discrimination claims against Dillard's. Dillard's moved to compel arbitration on the basis of the electronically signed employee arbitration agreement. Ms. Kerr denied ever having signed the arbitration agreement or having received the confirming e-mail.

Unfortunately for Dillard's, its system did not adequately address the authentication and repudiation risks because it could not show that only Ms. Kerr had access to her account. Therefore, Dillard's was unable to meet its burden of proof *at trial* to show, by a preponderance of the evidence, that Ms. Kerr knowingly and intentionally executed the arbitration agreement.[30] While the court did not accuse Ms. Kerr's supervisor of signing the arbitration agreement, it recognized that such a scenario was at least possible, or even that Ms. Kerr may have accidentally executed the arbitration agreement herself, thereby not knowingly and intentionally signing it.[31] Dillard's might have overcome this if it could have shown that Ms. Kerr had adopted the system, but, since Ms. Kerr had only accessed the system on three occasions over a period of at least five months, it was unable to do so. Since Dillard's failed to meet its burden of proof at trial, the court denied its motion to compel Ms. Kerr to arbitrate her employment claims and the litigation continued, in the precise forum the employer sought to avoid.

Verizon v. Pizzirani: Repudiation Can be Overcome if Opportunity to Review and Assent is Given

Verizon Communications v. Pizzirani demonstrates that when an employer can show a properly designed and risk mitigating HRIS, a court is more likely to bind the employee to terms, conditions or changes in employment communicated through the HRIS.[32]

Plaintiff Verizon sued Mr. Pizzirani, a former highly compensated executive in Verizon's broadband division who had resigned to work for a Verizon competitor, Comcast. Verizon sought enforcement of a 12-month noncompetition restrictive covenant that Mr. Pizzirani had received in an e-mail as a participant in Verizon's Long Term Incentive Plan, which awarded Verizon employees with both Restricted

Stock Options and Performance Stock Units ("Awards"). Mr. Pizzirani, as an Award recipient, had been advised in bolded language through e-mails from Verizon's human resources department in 2005 and 2006 of the following terms and conditions relating to his acceptance of the Awards:

> As you access you [sic] award on-line, it is important that you read and understand the terms and conditions of the Award Agreements. When accepting your award on-line, you acknowledge that you have read both the award agreements and Plan document, including the terms [and] conditions regarding vesting, restrictive covenants and the provisions concerning award payouts.[33]

On March 17, 2005, Mr. Pizzirani clicked on the "I ACKNOWLEDGE" button on the bottom of the e-mail, whereby he acknowledged that he understood that, in accepting such Award, he would be bound by the non-competition restrictive covenant. In 2006, however, Mr. Pizzirani did not click on the "I ACKNOWLEDGE" button, which resulted in the HRIS informing human resources that Mr. Pizzirani had failed to acknowledge.

In response to a call from Verizon's human resources, Mr. Pizzirani drafted and sent the following e-mail to an employee in the human resources department: "John I will read and agree to the terms and conditions of the award agreement and Plan documents."[34] After Verizon's human resources department received the email certification that Mr. Pizzirani had read and understood and agreed to the terms of the Award, that department granted Mr. Pizzirani access to the agreement on-line where he acknowledged and agreed to all terms.

In his defense, Mr. Pizzirani did not contest that he had executed the Award Agreements by electronic signature, but instead claimed that he did not read the contracts prior to electronically signing them and asserted that he was completely unaware of the restrictive covenants contained in them until October 2006. In essence, Mr. Pizzirani attempted to repudiate the terms of his agreement by claiming he never read them.

The court refused, enforcing the non-competition agreements against Mr. Pizzirani and barring him from accepting a competitor's offer of employment. The court recognized that, under "New York law, a valid contract is formed by manifestation of assent, including checking a box or clicking a button on a computer screen, as in this case[,]"[35] and that "parties are bound by the contracts they sign, whether or not the party has read the contract so long as there is no fraud, duress or some other wrongful act of the other party."[36] The court also stated that Mr. Pizzirani had a reasonable opportunity to know the essential terms and character of the agreements, Verizon encouraged him to read them, and he was adequately warned by e-mail that, through his acceptance, he certified that he had read, understood and agreed to be bound by the agreements and restrictive covenants.

Mr. Pizzirani also complained that he was only able to view the document in a small box on the computer screen, but Verizon demonstrated that its system gave Mr. Pizzirani the ability to print the agreements, save them to his hard drive or expand the default size viewing screen. The court also found it compelling that Mr. Pizzirani had no time pressure to read and sign the agreements. Verizon gave him more than a month to read and electronically sign the documents.

Because Verizon went to great lengths to ensure that its employees understood the importance of reading the documents, the court found little evidence that Verizon intended to misrepresent the terms of the Award Agreements.

Bell v. Hollywood: The Employer's Evidence of Knowing & Voluntary Consent Binds Employee

Bell v. Hollywood Entertainment Corporation presents another example of an HRIS that did address the risks raised in the *e*-Risk Analysis Framework. In that case, the court granted the employer's motion to compel the employee to arbitration because the HRIS effectively communicated to Ms. Bell the requirement that she arbitrate all employment disputes.[37] There, Ms. Bell completed her employment application process electronically either through a Hollywood in-store kiosk or over the Internet through Hollywood's Web site. Hollywood's application process required, as a condition to Ms. Bell's employment, that she agree to submit all claims involving workplace disputes to binding arbitration.

Ms. Bell later commenced an action against Hollywood for maintaining a hostile work environment, allowing sexual harassment to occur in the workplace and for civil battery. As Mr. Campbell had argued against General Dynamics, and Ms. Kerr against Dillard, Ms. Bell argued that she had received inadequate notice from Hollywood concerning the requirement that all of her workplace employment claims be resolved through binding arbitration. Unlike in the other cases, however, the court in *Hollywood* found for the employer, holding that Ms. Bell had agreed to arbitrate her workplace disputes because Hollywood could show, conclusively, that Ms. Bell had received information about the arbitration policy, provided evidence that she read and understood the terms and conditions of the policy, and that she had agreed to be bound to them as a condition of her employment.[38] The appellate court affirmed the lower court's decision to compel arbitration because it found that Ms. Bell "had the legal capacity to contract, signed the agreement and was sufficiently informed regarding the program. She was informed on how to obtain additional information, confirmed that she understood how to obtain additional information, and knowingly and voluntarily consented to arbitrate her employment claims against [Hollywood]."[39]

In analyzing the risks identified in the *e*-Risk Analysis Framework, one need only look to the factors relied upon by the court in reaching its decision. To minimize repudiation, Hollywood, in its electronic application process, presented Ms. Bell with a screen that informed her that all claims would be submitted to arbitration pursuant to Hollywood's Employment Issue Resolution Program (EIRP), with a link to a summary of the EIRP Rules or, if Ms. Bell desired, a link to a Web site containing a full copy of the rules and required that Ms. Bell either acknowledge or deny that she knew how to access the connecting links. The Hollywood system also minimized repudiation by requiring Ms. Bell to choose "yes" or "no" in response to her consent to arbitrate any and all employment disputes with Hollywood, thereby confirming her agreement. Finally, Hollywood's system also forced Ms. Bell to confirm that she knew how to access Hollywood's Web site to obtain the complete arbitration policy (even though there was no apparent evidence she actually reviewed such policy).[40]

The lesson of *Bell v. Hollywood* for employers looking to implement an HRIS is the same as that discussed above, in connection with *Campbell v. General Dynamics* and *Kerr v. Dillard*: employers must design and implement their system so it mitigates the preventable risks. ■

EXHIBIT 1

Use the e-Risk Analysis Framework to Identify and Mitigate the Risks Associated with the Design and Implementation of an HRIS

The *e*-Risk Analysis Framework is designed to assist employers in identifying and mitigating the six principal risks of an HRIS. The mitigation of these risks will help employers avoid the sorts of issues raised in the *Campbell v. General Dynamics*, *Kerr v. Dillard*, *Bell v. Hollywood* and *Verizon v. Pizzirani* cases, and should allow employers to conclude, as we do from our own experience with our clients, that companies can, through the use of a well thought-out HRIS, actually design and implement a system that equates with, and in many cases reduces, the risks associated with having employees continue to sign notices, acknowledgements or agreements in wet ink, and then storing those documents in hard copy.

NOTES

1. The term HRIS is used broadly to include any electronic computerized system that lets employers and employees interact on employment related issues.
2. Employer-employee notices, policies, disclosures and agreements will be collectively referred to as "agreements" throughout this article.
3. Locke Lord Bissell & Liddell LLP has developed the Six Point e-Risk Analysis Framework through its work in helping clients identify and mitigate the risks in moving to e-process solution.
4. Problems such as lost or unsigned signature pages, pen and ink modification to agreements, lost, missing or misplaced pages and/or personnel files, all become problems of the past, or, more appropriately, problems of the paper and wet ink world.
5. Campbell v. General Dynamics Government Systems Corp., 407 F.3d 546, 16 A.D. Cas. (BNA) 1361, 151 Lab. Cas. (CCH) P 60002 (1st Cir. 2005); Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648 (E.D. Pa. 2006); Bell v. Hollywood Entertainment Corp.,, 2006-Ohio-3974, 2006 WL 2192053 (Ohio Ct. App. 8th Dist. Cuyahoga County 2006); Kerr v. Dillard Store Services, Inc., 2008 WL 687014 (D. Kan. 2008).
6. Readers should also note that contractual enforceability is governed by state law, regardless of whether the dispute is heard in federal or state court. Nearly all states require the same three elements for the formation of a contract: (1) a meeting of the minds, (2) an offer and acceptance, and (3) the exchange of consideration (the exchange of something of value).
7. Many states have adopted rules of evidence that track the Federal Rules of Evidence (FRE). For purposes of this article all cited cases are based on the FRE or state law that follows the FRE. This article does not address admissibility concerns beyond legal authentication.
8. Repeated use of the same or similar signing ceremonies will also greatly contribute to the admissibility of documents signed using an HRIS.
9. This would require the employer to provide a witness with personal or expert knowledge to testify (in person or via affidavit) as to how each document was presented, signed, secured after signature to render it unalterable without detection, archived, retrieved and printed. This person will also testify as to the integrity and security of each system involved in creating, securing, archiving, retrieving and printing the document and should be qualified as an expert in that field.

10. See also Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 541-542, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).
11. State v. Swinton, 268 Conn. 781, 812, 847 A.2d 921 (2004) (applying the federal standard to a state case.)
12. State v. Swinton, 268 Conn. 781, 813, 814, 847 A.2d 921 (2004) (applying the federal standard to a state case.)
13. Magistrate Judge Paul W. Grimm's opinion in *Lorraine v. Markel American Insurance Company* provides ones of the best analyses to date of the admissibility of electronic evidence, which broadly could include electronic signatures. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 542, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007). *See, e.g.*: In re Vee Vinhnee, 336 B.R. 437 (B.A.P. 9th Cir. 2005) (proponent failed to properly authenticate exhibits of electronically stored business records); U.S. v. Jackson, 208 F.3d 633, 638, 53 Fed. R. Evid. Serv. 1030 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization's Web site); St. Luke's Cataract and Laser Institute, P.A. v. Sanderson, 70 Fed. R. Evid. Serv. 174 (M.D. Fla. 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); Rambus, Inc. v. Infineon Technologies AG, 348 F. Supp. 2d 698, 66 Fed. R. Evid. Serv. 16 (E.D. Va. 2004) (proponent failed to authenticate computer generated business records); Wady v. Provident Life and Accident Ins. Co. of America, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's Web site because affiant lacked personal knowledge); Indianapolis Minority Contractions Association, Inc. v. Wiley, 1998 WL 1988826 at *7 (S.D. Ind. 1998), judgment aff'd, 187 F.3d 743 (7th Cir. 1999) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them)."
14. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 544, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).
15. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 549, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).
16. State v. Swinton, 268 Conn. 781, 811, 847 A.2d 921 (2004).
17. Edward J. Imwinkelried, *Evidentiary Foundations*, 58-59 (LexisNexis 6th ed. 2005).

    1. The business uses a computer.
    2. The computer is reliable.
    3. The business has developed a procedure for inserting data into the computer.
    4. The procedure has built-in safeguards to ensure accuracy and identify errors.
    5. The business keeps the computer in a good state of repair.
    6. The witness had the computer readout certain data.
    7. The witness used the proper procedures to obtain the readout.
    8. The computer was in working order at the time the witness obtained the readout.
    9. The witness recognizes the exhibit as the readout.
    10. The witness explains how he or she recognizes the readout.
    11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

18. In re Vee Vinhnee, 336 B.R. 437, 447 (B.A.P. 9th Cir. 2005). Opposing parties often allege that computer records have been tampered with and thus lack authenticity. Such claims have been viewed as "almost wild-eyed speculation… without some evidence to support such a scenario…." U.S. v. Whitaker, 127 F.3d 595, 602, 47 Fed. R. Evid. Serv. 1197 (7th Cir. 1997).
19. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 549, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).
20. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007), quoting *Weinstein's Federal Evidence* § 900.07[3].
21. Lorraine v. Markel American Ins. Co., 241 F.R.D. 534, 552, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007).
22. Federal Rules of Evidence 902 (11).
23. Federal Rules of Evidence 902 (11) at 773 at footnote 4.
24. A regulatory violation does not necessarily void an agreement, or even make it voidable, but may just lead to penalties or fines.
25. Campbell v. General Dynamics Government Systems Corp., 407 F.3d 546, 16 A.D. Cas. (BNA) 1361, 151 Lab. Cas. (CCH) P 60002 (1st Cir. 2005).
26. Campbell v. General Dynamics Government Systems Corp., 407 F.3d 546, 558, 16 A.D. Cas. (BNA) 1361, 151 Lab. Cas. (CCH) P 60002 (1st Cir. 2005).
27. Campbell v. General Dynamics Government Systems Corp., 407 F.3d 546, 555, 16 A.D. Cas. (BNA) 1361, 151 Lab. Cas. (CCH) P 60002 (1st Cir. 2005).
28. Kerr v. Dillard Store Services, Inc., 105 Fair Empl. Prac. Cas. (BNA) 1298, 92 Empl. Prac. Dec. (CCH) P 43483, 2009 WL 385863 (D. Kan. 2009).
29. The Dillard Department Store is commonly referred to as Dillard's, so other than in the case name, we use that vernacular.
30. Kerr v. Dillard Store Services, Inc., 105 Fair Empl. Prac. Cas. (BNA) 1298, 92 Empl. Prac. Dec. (CCH) P 43483, 2009 WL 385863 (D. Kan. 2009).
31. Kerr v. Dillard Store Services, Inc., 105 Fair Empl. Prac. Cas. (BNA) 1298, 92 Empl. Prac. Dec. (CCH) P 43483, 2009 WL 385863 (D. Kan. 2009).
32. Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648 (E.D. Pa. 2006).
33. Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648, 652 (E.D. Pa. 2006).
34. Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648, 653 (E.D. Pa. 2006).
35. Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648, 655 n.3 (E.D. Pa. 2006).
36. Verizon Communications Inc. v. Pizzirani, 462 F. Supp. 2d 648, 655 (E.D. Pa. 2006) (internal quotations omitted).
37. Bell v. Hollywood Entertainment Corp., 2006-Ohio-3974, 2006 WL 2192053 (Ohio Ct. App. 8th Dist. Cuyahoga County 2006).
38. Bell v. Hollywood Entertainment Corp., 2006-Ohio-3974, 2006 WL 2192053 (Ohio Ct. App. 8th Dist. Cuyahoga County 2006).
39. Bell v. Hollywood Entertainment Corp., 2006-Ohio-3974, 2006 WL 2192053 (Ohio Ct. App. 8th Dist. Cuyahoga County 2006).
40. The *Bell v. Hollywood* court even quoted from *Campbell v. General Dynamics*, in noting that a "signature may not be denied legal effect or enforceability solely because it is in electronic form … [and a] contract may not be denied legal effect or enforceability because an electronic record was used in its formation."