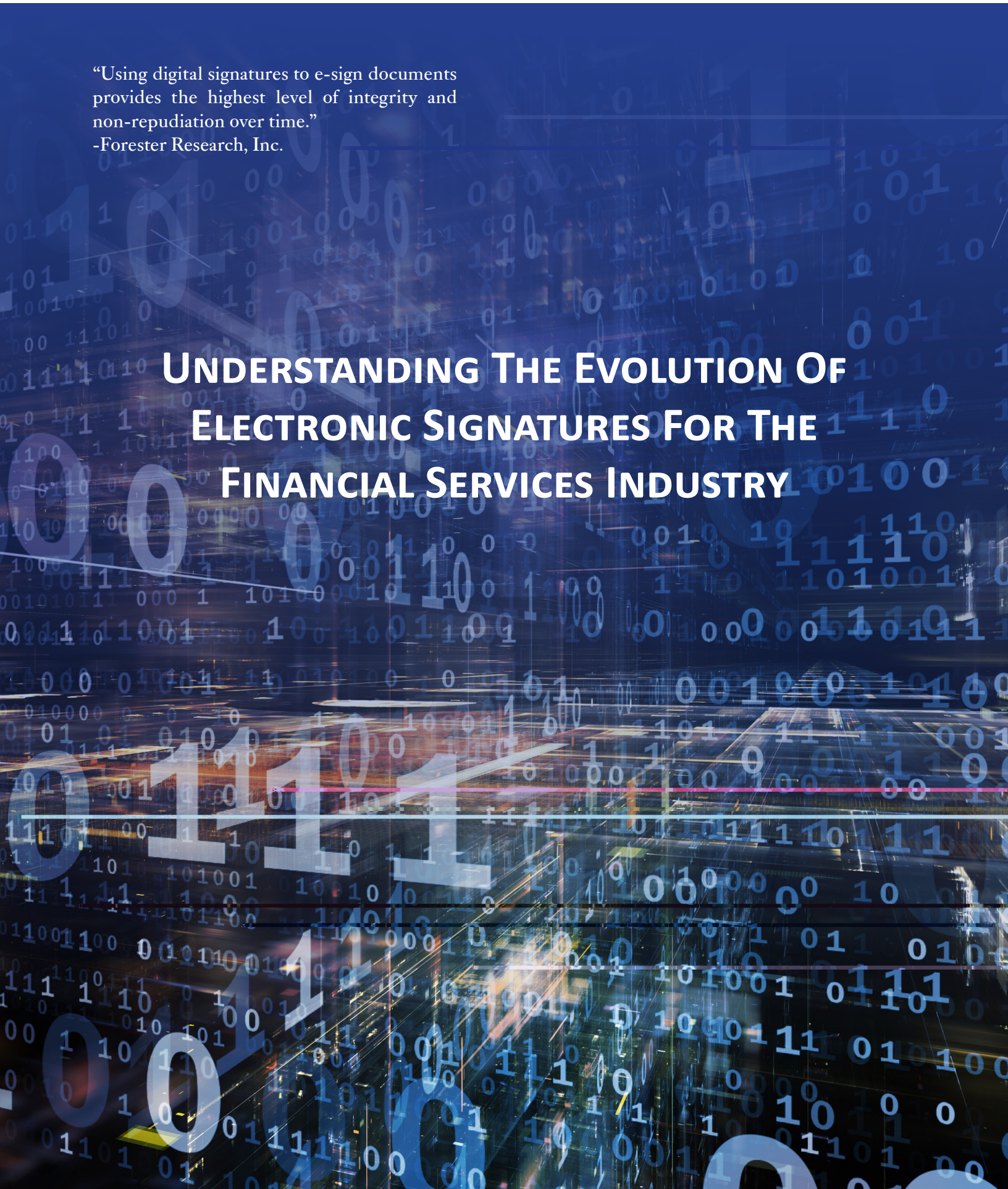
Docupace
TECHNOLOGIES

"Using digital signatures to e-sign documents provides the highest level of integrity and non-repudiation over time."
-Forester Research, Inc.



Understanding The Evolution Of Electronic Signatures For The Financial Services Industry

In today's financial world, secure and compliant electronic processing can transform a business and positively impact workflow efficiencies as well as business enhancements.

At Docupace Technologies, as leaders in this field of secure & compliant electronic processing, we felt it our responsibility to share our knowledge regarding the evolution of e-signatures, information on the laws and regulations, as well as the resulting workplace productivities and the protection of the ever-growing data files that are a reality in the majority of businesses.

Our white paper, entitled the Understanding The Evolution Of E-Signatures is just that--our effort to educate readers on the importance of being familiar with the compliance issues associated with e-signatures and how to navigate the complexities surrounding the electronic processing platform for financial institutions and wealth management firms.

The securities industry has always had a compelling need for e-signatures and paperless processing. Now this compelling need has come full circle with regulatory guidance and the technology that makes this possible.

Our collective team of experts at Docupace, present this white paper to help answer your questions and clarify issues needed to promote workflow solutions.

Sincerely,
Michael Pinsker
CEO

Table of Contents

Consider This:

You run a financial services firm. The company has grown over the past few years and you anticipate it will continue to grow. That growth poses a challenge: how will you handle and manage all the paper involved and still remain in compliance with record retention that results from company growth? You could add staff, but that would increase costs. You could expect your field employees to do more of the client management functions remotely, but that will probably result in employee pushback or visible frustration.

Or, you could invest in technology to streamline your processes and adopt e-signatures, which would reduce the amount of paper being transmitted between the field and the home office, reduce the staff time required to open new accounts and likely result in happier clients and employees, while reducing your over all cost.

The Evolution of Signatures

Electronic signature legislation is evolving the way business and commercial transactions are conducted. With the rise in electronic communication and desire among many to "go paperless," it was only a matter of time before signing paper to indicate your agreement or approval of something would become an antiquated process. So called "wet ink" signatures, when pen is applied to paper considered the antiquated process, is still the de-facto standard in many industries, including financial services, but there are far better options today that allow for efficiencies, productivity and security.

E-signatures are defined as a "sound, symbol or process, logically associated with a document" such that it is:

1. Unique to the user
2. Under the sole control of the signer
3. Linked to a document in such a way as to prevent tampering and
4. Capable of being authenticated

Digital signatures are based on Public-Key Infrastructure (PKI) technology and assure the highest level of security. Digital signature technology has been used for decades, which means it is highly standardized and accepted. A digital signature essentially links a "fingerprint" of the document at the time of signing with an identity credential (a digital certificate), and the result is permanently embedded into the document. A digital signature proves integrity by clearly showing when a document has been changed or tampered with. The signature also uniquely identifies the signer and can provide additional information about the time of signature, providing significant non-repudiation.

Electronic signatures are commonly used for financial transactions and in other cases where it is important to detect forgery or tampering.

Defining the Terms

The terms "electronic signature" and "digital signature" are often used interchangeably but they are quite different. An electronic signature is any identification and verification method used in an electronic version of a document, such as a scan of your hand-written signature or an electronic authenticity stamp. An electronic signature may be in the form of a bitmap or picture that can easily be cut and pasted. The electronic signature is simply data in electronic form, which are attached to, or associated with, other electronic data and which serve as a method of authentication. A digital signature accomplishes the same purpose—signing a document—but uses various encryption methods for added verification and security. Put another way: all digital signatures are electronic signatures, but not all electronic signatures are digital signatures.

When using electronic signatures, the process can be completely paperless. A document requiring a signature is uploaded to one of the many e-signature providers' online system. It is tagged with annotations noting where signatures or initials need to be inserted. The file is sent to the signer, who "signs" it using a few mouse clicks with an electronic version of their signature. When everything is signed or initialed, it is sent back to the sender. And there it is! Transaction complete.

Benefits and Challenges of Signature Types

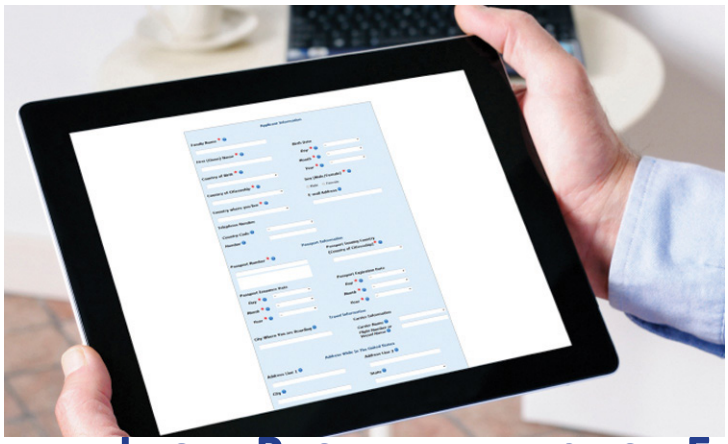
Of course, each type of signature—wet ink, digital and electronic—offers benefits and challenges. Wet ink signatures are still considered the gold standard, partially because that's the way things have been done for so long. The signer's identity is usually verified by photo, the signature compared to a verified sample and you're done. The challenge comes in storing and maintaining the signature for the long-term. Original documents take up space and can decay, it can be difficult to find hard copies when subject to an audit and it can be costly to store many years' worth of files.

Digital Signatures

Digital signatures travel with the document and are based on industry and international standards, so they can be verified independently without requiring the document to check back with a server. Digital signatures are also more widely accepted internationally than electronic signatures. However, digital signatures have been avoided historically because they require a significant investment to implement and often require users to carry hardware tokens or smart cards to securely store their signing credentials.

Electronic Signatures

E-signatures are rising in popularity and hold up in court as being equivalent to wet ink signatures. The reduction in paper and possible human error, coupled with secure and compliant storage, are big benefits to any industry that handles a lot of paper. One challenge is in ensuring the signer's identity, which is why notary publics are used with wet ink signatures. There isn't yet a good alternative to a notary for e-signatures, so some transactions will require both an e-signature and wet ink signature. That being said, many financial services and other professional services firms are moving to implement e-signatures.



Regulatory and Legal Requirements for E-Signatures

Compliance is perhaps the most important reason to integrate e-signatures with the rest of a paperless office. There are a multitude of legal and regulatory rules, requirements and guidelines for e-signatures. Understanding government and industry regulation will help users apply best practices when using e-signatures.

What Federal Standards Are in Place? The Electronic Signatures in Global and National Commerce Act (ESIGN) was adopted by Congress, signed by the President and took effect October 1, 2000. ESIGN applies throughout the United States and adopts the relatively simple principle that electronic signatures and records should be accorded the same legal status as wet ink signatures and paper records. Importantly, ESIGN does not change the underlying substantive provisions of the laws within its scope; it simply affects the medium for execution and delivery of writings.

ESIGN spells out a specific set of disclosures, which must be provided to consumers as a condition to accessing the benefits of ESIGN. These disclosures, delivered during the first enrollment and consent, permit consumers to later withdraw their consent to do business electronically.

In concert with ESIGN, The Uniform Electronic Transactions Act ("UETA") has been adopted in 49 jurisdictions. Every state except Illinois, New York and Washington has adopted a variation of UETA. These three states have adopted their own unique alternative statues. This has empowered parties to most transactions to do business electronically, confidant that their contracts are legally enforceable.

UETA is built on three rules:

- A record or signature may not be denied legal effect of enforceability solely because it is in electronic form
- If a law requires a record to be in writing, an electronic record satisfies the law and
- If a law requires a signature, an electronic signature satisfies the law

UETA does not change the existing common law rules concerning contested signatures and the burden of proof. If the authenticity of an electronic signature is disputed, the person seeking to enforce the signature is required to prove that the signature was executed by the person

against whom enforcement is sought. This means that parties accepting electronic signatures must satisfy themselves that the signatures are sufficiently verifiable, under the circumstances and for the contemplated purpose, to counterbalance the risk of a dispute. UETA's E-Signature Guidelines also retains the common law requirement that a signature, to be valid, must be the intentional act of the signer.

What are the SEC/FINRA Rules?

Since 1939, the SEC has required broker-dealers to create and maintain certain records to ensure compliance with federal securities laws and regulations (Rule 17a-4(f)). To meet the demand for electronic document storage, Rule 17a-4(f) was adapted to include regulations for electronic records in 1997. These requirements are designed to make sure electronic records are accurate and accessible. The Rule's transition from an exclusively paper process to its current state reflects the SEC's attitude of promoting emerging technologies to benefit broker-dealers and investors. Rule 17a-4(f) requires that document storage must prevent the document's contents from being erased, overwritten or altered.

In 2001, the Securities and Exchange Commission (SEC) published guidance on electronic signatures (17 CFR Part 241) for the securities industry to ensure accuracy, accessibility and accurate reproduction of e-signatures. Each valid e-signature must be associated with a transaction record and executed or adopted by a person with the intent to sign. This means that a valid e-signature under the law can't be:

- Signed or stored separately—for example, on a blank sheet of paper—apart from the transaction record
- "Robo-signed" by a computer (not a person)
- Signed deceptively, copied or commingled

When the ESIGN Act was enacted in 2000, the SEC released a statement about the use of electronic signatures (Release No. 34-44238) to clarify how the new technology would work within the electronic records rules already in place.

The release supported the regulations of ESIGN and stated that electronically signed documents that comply with the ESIGN Act would also be SEC-compliant as long as they comply with the document retention requirements of Rule 17a-4(f).

ESIGN requires consumer protections for documenting and protecting proof of transaction and delivering and storing related consumer disclosures. Prior to obtaining an electronic signature and consent, the party to the transaction must be provided with all disclosures otherwise required for the transaction. Disclosures must be delivered at or prior to the electronic signature in compliance with ESIGN and SEC rules. All required disclosures must be delivered. For example, by electronically establishing an account with an electronic signature, the dealer firm/financial adviser must confirm that it has provided the investor a copy of the document, applicable fund prospectuses, Traditional and Roth IRA Disclosure Statement and College America Program Description, if applicable, and any other materials that may be required in connection with the establishment of the account on behalf of the adviser's client. The adviser's investor must also read and agree to the terms of

these documents prior to electronically signing.

Disclosures may require specific consent in addition to the e-signature consent. Generally, the party must be given a clear and conspicuous statement informing them:

- They have the option of having the record available on paper or non-electronic form
- A description of the transaction or types of transactions covered by the consent
- The right to withdraw consent and the procedure for doing so
- How the consumer can request a paper copy of the record and information of any charges that apply
- How the consumer can update contact information and
- The hardware and software requirements for receiving the disclosures electronically

FINRA also uses the guidelines of ESIGN to determine if an electronic signature is compliant. The agency considers valid electronic signatures to be any electronic mark that clearly identifies the signer and is otherwise in compliance with the ESIGN Act, the SEC's guidance about the ESIGN Act and the advice provided through FINRA's interpretive letters. These interpretive letters require that financial advisors:

- Be capable of indexing and cross-referencing stored information to ensure access to all relevant documents and records
- Store documents in a non-rewriteable and non-erasable format
- Will allow for third-party access to their documents

Challenges to E-Signature Acceptance

Even with all the benefits that e-signatures offer, there are some challenges to industry-wide adoption. The two main obstacles for adopting e-signatures within the financial services industry are receiver reluctance and lack of industry standards for integrated paperless processing.

Financial services firms are reluctant to adopt e-signatures, despite customer demand for paperless processing and e-signatures. This is mainly because some receivers of data are not yet accepting proven technologies. These receivers include clearinghouses, mutual fund groups, hedge funds, private placement providers and direct participation programs. Some companies have been proactive in adopting e-signatures, while others are hesitant. Until broker dealers can be confident that e-signatures and paperless processing are widely accepted, with any organization they work with, firms will not fully implement e-signatures.

The e-signature/paperless processing industry has spawned diverse vendors, technologies and standards. These demonstrate innovation but none are stand-alone solutions to make paperless processing simple and seamless. For example, a securities representative can purchase an electronic signature pad "off the shelf" and start using it to capture client signatures electronically. It would seem to be a first step in paperless processing, but the pad alone doesn't begin to meet ESIGN requirements or industry standards, much less compliance requirements. No stand-alone pad can track the full life cycle of a transaction and bind an authentic signature to that particular transaction, securely and forever.

Above the enterprise-level, the securities industry also has integration challenges, which can be solved with uniform industry standards to connect vendors and technologies. The securities industry currently lacks a "Universal Connector" software standard to make sure that leading paperless solutions work together.

Compliant E-Signature Solutions

While there is no software standard, there are e-signature services that fully comply with ESIGN, as well as SEC/FINRA regulations. Three separate formats of ESIGN-compliant signature technologies have emerged in the securities industry:

- Digital or electronic stamp used by a known person
- Electronic signature pads
- Remote signing through multi-factor authentication

Which is best? What are the differences?

Example of the Process

- A document or transaction is reviewed by the signer(s)
- The signature is captured in the presence of the advisor/representative, using that individual's bound signature pad or tablet
- The signature is bound to a fillable electronic PDF document via cryptographic hashing via the AutoKey generation and EncryptionMode functions of Adobe controls
- The Signature and Key receipts are obtained from the control and concatenated together to form a Transaction Receipt
- Transaction documentation is then printed or emailed to the client. The client can verify that the document and signature match those displayed by the application. The transaction receipt, the signature and the document data are stored as evidence of the completed transaction.

Digital or Electronic Stamp Used by a Known Person

This format is used to authenticate advisor/producer signatures and for principal approvals. The firm assigns a unique electronic stamp to each known person and that, stamp may be used by that person, either physically (in-person) or remotely. Since clients and prospects are not considered "known persons," this format may not be used for consumer signatures.

Electronic Signature Pads

A hardware device, similar to those used in store checkout lines, is used to create a biometric record of the client's physical signature, including signing speed and pressure. Each pad is "bound" to a unique advisor/producer and requires individual authentication. Topaz Systems, Inc. is a leader in supplying signature pad hardware for the financial services industry. (Note: Security for a tablet used in a store checkout is not as robust as in those used by financial services firms.

If a dispute arises, the stored contract and signature are used to re-generate the receipts. The receipts are then compared to the stored receipts and can be compared to the printed receipt that was provided to the signer at the time of signing. The comparison of the stored receipts to the regenerated receipts from the e-contract protects the firm against customer repudiation and proves that the document and signature are the same as originally signed.

If the signer claims that the signature is a forgery, the bound signature and document data can be provided to a forensic document examiner utilizing the tablet's analysis tool and a handwriting analysis expertise to authenticate the identity of the signer. The signature and document receipts are unique to the original document and signature, and the storage of receipts allows for conclusive comparisons at a later date. Validation of the transaction through multiple receipts prevents forgery from going undetected. With reliable receipt storage, it is impossible to modify the document and fool this kind of system, which protects both the firm and client.

Multi-Factor Authentication

Like electronic pads, this format may be used for customer signatures, provided that the documented steps are taken to authenticate information available exclusively to the signer. This format may be use remotely as well as in-person. It may appear expensive to implement a secure authentication mechanism to manage subsequent signing, client communication and document distribution—but the cost is far less than advisors are currently spending for printing, copying, mailing and tracking documents.

As an example, a leading provider of e-signature technology has developed a consumer interface for a remote signing process with multi-factor authentication. The consumer adopts a signature and initials, which are then authenticated and used on all subsequent transactions requiring a signature.

"It may appear expensive to implement a secure authentication mechanism to manage subsequent signing, client communication and document distribution—but the cost is far less than advisors are currently spending for printing, copying, mailing and tracking documents. "

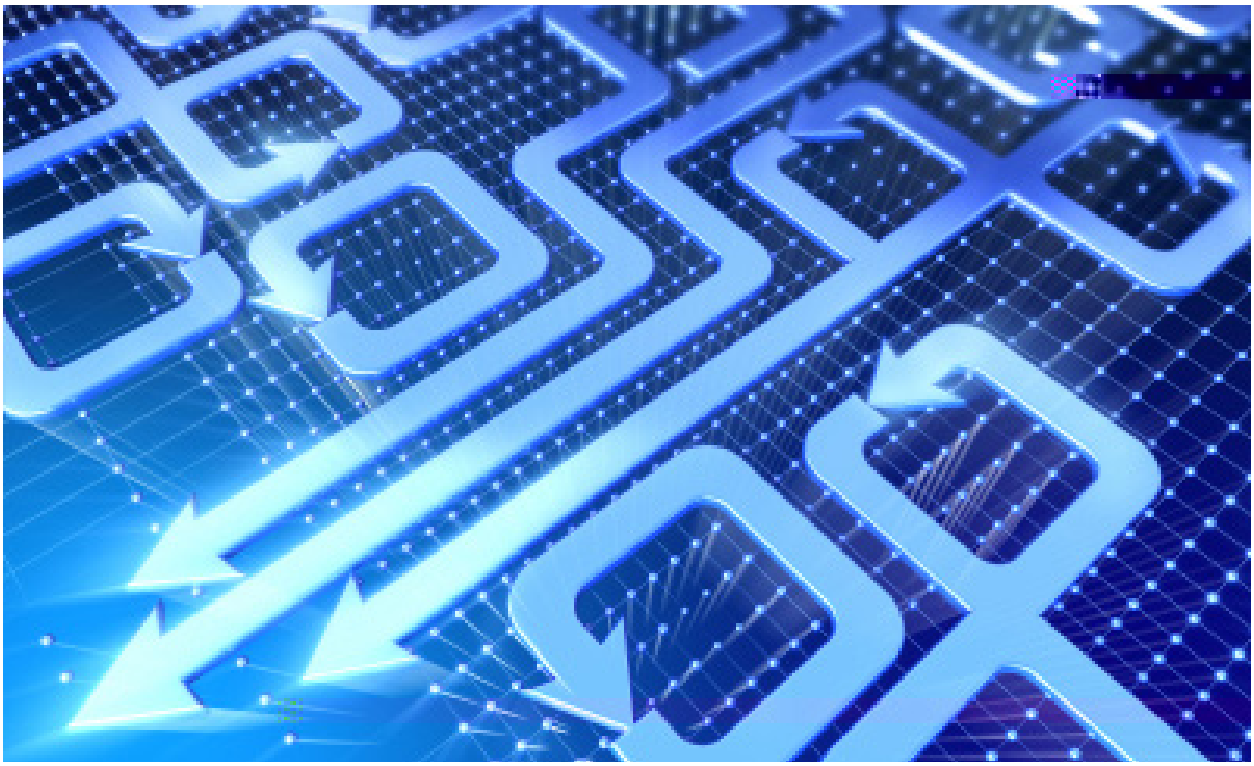
Financial services firms still need to support wet ink signatures as the evolution to paperless records and e-signatures unfolds. Specific types of documents, such as stock certifications and medallion-stamped documents, cannot be processed with e-signatures. To convert wet ink signatures to electronic signatures (where applicable), the hard-copy document is scanned at the branch or broker-dealer level and then either shredded or forwarded. If a wet ink signature is forwarded, it is typically sent to a third party outside of the broker-dealer, such as a clearing house or transfer agent. Regardless of which format is used, the goal of an electronic signature-capture system is to reproduce the techniques, ceremony, familiarity and convenience of handwritten signatures on paper.

The Industry

An emerging industry leader in delivering SEC/FINRA compliant paperless processing systems to financial services firms is Docupace Technologies LLC, which is also leading the charge in helping the securities industry establish an industry standard, the aforementioned "Universal Connector." Further it is helping product sponsors (mutual fund companies, insurance carriers, REITs, etc.), broker-dealers and advisors establish a transparent level of trust between each other as well as the end consumer, through accommodating all of the various signature methods in accordance with SEC/FINRA regulation.

The Docupace STP Network©

As a hub of secure paperless processes, Docupace STP Network© is accessible by all users of forms, documents and data including clients, advisors, broker-dealer's home office, product companies and clearing firms. Delivering the industry's first web-based SEC/FINRA compliant paperless processing system, its document management and workflow solution simplifies the process of capturing, organizing, routing and accessing information. Docupace's



e-signature solution exceeds the requirements of ESIGN, FINRA rules and SEC requirements by utilizing electronic signature pads or remote signing through multi-factor authentication processes and by providing all disclosures in compliance with ESIGN and SEC rules.

ePACS is Docupace's web-based, electronic, straight-through processing app providing fully integrated document management and dynamic workflow, e-signatures, e-forms, an option for web service integration with vendors and Check21 processing. The Docupace system eliminates rework and improves data integrity, substantially reducing NIGO rates. CRM integration automates form-filling, assuring "once-and-done" data entry and a completely electronic process. This is a huge cost saver.

"Docupace STP Network©, has developed the proprietary mechanism to accommodate all types of signatures—wet ink signatures, e-signatures and digital signatures."

And, from the client's perception, less mistakes mean more trust.

Firms using the Docupace system are provided with rich data points that allow users to model, measure and manage their business according to the numbers. The workflow monitor and reports will give you a 360-degree view of KPI's to drive continuous process improvement. This helps firms and advisors alike grow and build their businesses.

A centralized SEC/FINRA compliant WORM repository allows secure access to all workflows, business processes, and documents. Robust search capabilities allow for federated searches across the entire repository. Multiple layers of physical security and proprietary technology coupled with the most secure data center on the planet provide peace of mind.

Benefits of the Docupace STP Network© include:

- Faster and More Compliant Transactions—Digital signatures help get client signatures on investment documents in minutes instead of days or even weeks. And unlike paper documents, Docupace can designate mandatory fields, resulting in 100% complete documents every time. That means one never needs to track down clients and have them re-send or re-sign documents.
- Clients and Advisors Connect—Clients and broker dealers can sign documents anytime, anywhere, on any device, offering a faster and easier method of interaction.
- Straight-Through Processing Is Enabled—All documents, data and signatures can connect to client's back-end system and be routed to your intermediaries. This eliminates faxing, scanning and manual re-keying. And because data fields get collected, captured and verified at the point of signature, there is a visible drastic reduction in NIGO (Not In Good Order) documents.
- Costs Are Reduced—Digital signatures save financial advisors time by sending documents for signature instantly. This gives more time for relationship-building and sales, instead of paperwork. Not to mention the savings captured by reducing the need to print, copy, fax, mail and store paper documents.
- Best-in-Class Document Security—Digital signatures offer the highest possible level of document security. Signed documents are tamper-evident and come with a highly detailed audit trail, giving more than enough evidence in the event of arbitration.
- Dynamic workflow(s)—whether packaged out of the box or customizable to fit a client's business, both are available and remain in the client's control.
- Retrieving Documents—Clients know the status or work with the click of a couple buttons and thus can save hours searching for documents
- Reporting—Internal and external audits are realized by the reporting capabilities, reducing risk and gaining efficiencies.

And the Network's central repository allows you to aggregate all your documents in a disaster-proof virtual vault. The world's top 40 Internet providers converge at the SWITCH location in Las Vegas, NV, meaning Docupace traffic is routed based on the highest speed and availability. The system's logical security is powerful, flexible and battle tested.

Docupace STP Network©, has developed the proprietary mechanism to accommodate all types of signatures—wet ink signatures, e-signatures and digital signatures. Advisors initiate a request from within Docupace and send for signature by any of those signature formats. Once the request has been signed and approved, the request is automatically routed back into the proper client folder as a new version, within the Docupace SEC/FINRA Compliant repository. In every signing method, Docupace authenticates the user and method, whether it be as a known entity (person registered or employed by the broker-dealer) or a person authenticated with biometrics and/or challenge questions.

Secure E-Signatures

Docupace's e-signature solution is compliant with SEC and FINRA requirements. The firm also integrates with Topaz, for those representatives that want to use a signature pad. All electronic emails, notes, document annotations, etc. are considered client correspondence and are subject to Rule 17a-4(f) record keeping requirements as client correspondence. Documents must have a feature called "tamper evidence." If someone tries to change any part of the document (even something as simple as deleting a space or capitalizing a word), there's proof that tampering took place.

With Docupace digital signatures, documents are tamper-evident not just at the end of the signing process, but from the moment the transaction is started. This provides evidence that the first signer didn't alter the document before it was sent to the second signer. Because Docupace uses digital signatures for every single signature, intent and content integrity are built-in, showing a clear trail of the document's content from the first signature to the last. Using Docupace e-signatures ensures the highest possible level of compliance with regulators. Users click-to-sign, just like in an electronic signature solution, but behind the scene Docupace and its partners use high assurance digital signature technology for each and every signature.

And Now, E-Signature Adoption...

With so many considerations and regulations surrounding e-signature adoptions today, it is vital for advisors, broker dealer executives (CEOs, COOs, and CCOs), operations managers and product companies (mutual fund companies, insurance carriers, etc.) to be well informed as to the detailed guidelines needed to ensure that there is compliance with all rules and regulations

There is no question that e-signatures will become standard in the financial services industry, as they will in most other industries. The time is now.

THE GUIDELINES

These guidelines are intended for third party service providers, as well as internal developers and project managers.

Questions to ask:

1. Does the user have authority to sign the electronic record?
2. Does the system or process provide evidence of the user's intent to sign the record?
3. What is the method or process for attributing the signature to the user?
   a. How is the signer being authenticated prior to signing?
   b. What audit trail, log or other evidence links the authentication process to the signature?
4. Is the signature embedded in, logically associated with, or otherwise linked to the record being signed?
5. How is the record delivered and presented to the user?
6. What is the process for storing the electronic record?
   a. Does it prevent or allow for the detection of any alteration to the record after it has been signed?
   b. Who has access to the record?
   c. When/how is the signer provided an opportunity to retain the electronic record?

Electronic Signature Affirmations

- Affirming the accuracy of information in the Record ("By signing this form I acknowledge this Record contains the correct information")
- Affirming assent or agreement with the information in the Record ("I have agreed to the terms and conditions described in this Record, because I signed it")
- Affirming the signer's opportunity to become familiar with information in the Record ("I must have had this Record in front of me, because I signed it") or
- Affirming the source of the information in the Record ("This Record must have come from me, because I signed it")

Agreement to Transact Business Electronically

Transaction participants are not required by any rule of law to use electronic signatures. Therefore, a general agreement to use electronic records and signatures is a prerequisite to engaging in electronic transactions. In the event of a dispute, it will be important to establish that all transaction participants were willing to use and accept electronic signatures instead of handwritten signatures.

Adherence To ESIGN Rules

(transactions entered into for personal, family or household purposes)

- the consumer's affirmative consent must be obtained in accordance with the specific requirements of ESIGN. Note that ESIGN states that the legal effectiveness, validity or enforceability of any contract executed by a consumer will not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer. However, the failure to obtain effective ESIGN consumer consent may trigger penalties or remedies that apply under other law for failure to make proper disclosures or deliver required documents.

Advisors should scrutinize all the circumstances that may trigger a signature requirement to include giving of consent. Even if there is no requirement for a signed record, the investor should be given a meaningful opportunity to access the terms for doing business.

Electronic Signature Example

"By electronically signing this Agreement, I acknowledge and agree that such electronic signature is valid evidence of my consent to be legally bound by this Agreement and such subsequent terms as may govern the use of your services. I accept notice by electronic means as reasonable and proper notice, for the purpose of any and all laws, rules and regulations. I acknowledge and agree that ADVISOR may modify the Agreement from time to time and agree to consult ADVISOR'S website from time to time for the most up-to-date Agreement. The electronically stored copy of this Agreement is considered to be a true, complete, valid, authentic and enforceable record of the Agreement, admissible in judicial or administrative proceedings to the same extent as if the documents and records were originally generated and maintained in printed form. I agree to not contest the admissibility or enforceability of ADVISOR'S electronically stored copy of the Agreement."

If ESIGN consumer consent is required before

the documents can be delivered and the signatures obtained, the consent process must occur before delivery of the documents. The consent process should include:

- Electronic presentation of the required ESIGN consent disclosures
- An electronic consent from the consumer
- A reasonable demonstration of the consumer's ability to receive and review the records being delivered

Identification

- The parties to the transaction must be accurately identified.
- ESIGN does not address whether the signature may properly be attributed to a particular person; that is left to be determined by other laws and the surrounding factual circumstances.
- In disputes about the authenticity of an electronic signature, the burden of proof that the signature is genuine will be upon the person seeking to enforce it.
- The technology provider should be satisfied that electronic signatures are sufficiently verifiable, to counterbalance the risk of such a dispute.

Credentials Needed for Authentication

- Third party or positive proof of identity (such as a government-issued driver's license or passport) is required as part of authentication
- Supporting documents related to the authentication process (such as EXAMPLES) shall be obtained
- Full compliance with the USA Patriot Act is required

For signed records submitted by third parties or external vendors, the signed records should include a transaction summary that contains the audit trail in an agreed-upon format.

UETA Guidelines for Multiple Signers and Co-Owners

- Each signature must be accompanied by dates and other identifiers, to confirm the signature independent of other signatures. This is part of the content of the record and needs to be preserved, as lack of this information seriously affects a document's reliability and authenticity.
- In the event the automated document requires (i) multiple signatures (including initials) to one record by the same signer or (ii) a signer's signature to multiple records at the same time, the signature process must enable intent to be established for each signature.

Intent

- It must be clear that the signer intended to create a signature and, when not reasonably apparent, the signer should be advised that the signature fulfills one or more purposes.
- If the signature is disputed, the person attempting to enforce the signature will usually have the burden of proving the intent to sign, based on what a signer reasonably would have believed under the circumstances, and the signature's purpose.
- The system implemented to obtain the electronic signature must be compliant with all requirements for obtaining consent for e-delivery of documents as well as review and/or approval of necessary disclosure documents.
- All sections of the document requiring a signature, must be signed by the appropriate party.
- In cases where one party may be required to sign a single document in more than one place, a separate signature or evidence of intent to sign should be obtained for each location where a signature is required.
- If multiple documents are to be signed, a separate signature or expression of intent to sign must be obtained from the signer for each signature. Each party involved in the event (such as the establishment of the new account or transaction) will have their own set of credentials. Once issued, these credentials cannot be modified except via a structured process the system may provide for modifying or updating the credentials.

In many transactions, some of the document will be signed by more than one person. This usually will not present any special issues when the signing participants are accessing the record from different physical locations. However, when more than one participant is signing at the same location, certain electronic signature methods will not, in and of themselves, demonstrate that each signer created his

or her own signature. Of course, it will often be the case that the signing participant has actual or implied authority to sign on behalf of another. When this is not the case, the firm may wish to employ procedures, credentials and/or signature methods that will help establish that each required signature may properly be attributed to the nominal signer.

Each party may be provided with a unique PIN (personal identification number) to use for signing records in connection with the transaction. When it is time to sign the record, each party will be asked if they are ready to sign. If they click on the button marked "SIGN NOW", they will be asked to enter their PIN to complete the signature process. Once they enter their PIN, their signed record will be just as enforceable as a written document signed by hand. Each signer will have a separate PIN, which should not be shared with any other signer. Failing to keep the PIN secret could result in signatures being added to a record without the party's knowledge.

Authentication

For authentication purposes, the application of the e-signature may need to be captured in a manner that preserves the metadata directly associated with the signature for future reference. Audit trails must be maintained concerning the signing of the electronic record. Those audit trails must include the following, as applicable:

- Information on authentication of the signer, whether through successful use of a credential or otherwise
- Biometric recording, if a biometric signature has been used
- A record of the significant events in the record presentation and signing process, including the date(s) and time(s) on which the record is presented, reviewed and signed and
- Identification of the record to which the signature was applied

Document Integrity and Alterations (UETA)

Records that have "integrity" are records that are complete and have not been altered without proper authorization. Records must be protected against undetected and unauthorized alteration. Records management policies and procedures should specify:

- what, if any, additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them.
- Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as an annotation or addition. The structural integrity of records must also be maintained.
- The physical and logical format of the record and the relationships between the data elements comprising the record should remain intact. Failure to maintain the record's structural integrity may impair its reliability and authenticity.

When parties have signed documents or sections of documents electronically, the content cannot be modified without potentially voiding the signature or invalidating the document. Once the final signature has been applied, the document cannot be opened for changes, additions or deletions. For example, the following process should be followed when opening a new account:

- For transaction-specific documents that are electronically signed, visible information shall be contained in the signed signature field displaying the date the signature was applied to the document (for example, "Electronically Signed on this [date] at this [time] by [name of signer]")
- Procedures shall be adopted such that adviser's clients are not committed to the event (such as the establishment of a new account or transaction) until the final signature is applied. Further, adviser's clients shall be provided the entire document to review and retain regardless of how many instances of intermediate signatures have been applied prior to the final signing and locking of the document
- An appropriate audit trail should be established to track any alterations that have been made and who made them

Effective Delivery

Effective delivery of records is an important prerequisite to obtaining an enforceable signature. In general, delivery of a record occurs:

- At the time the record is displayed to the recipient, or at the time a notice is given to the recipient (i) with the record attached, or (ii) with a hypertext link to the record, or (iii) with other notice to the recipient advising of the record's location, as appropriate under the circumstances and based on any elections the recipient has made

- When delivery occurs via email attachment or email notice, prior agreement with the recipient is necessary to establish that the email address is valid and that it may be used to deliver records or notices.
- When delivering a record online, it is important to establish the appropriate timing for delivery and the length of time the record will be available for review.
- In some transactions, certain information must be presented at a particular time or as part of a specific step in the transaction.
- It is also often necessary for information to remain accessible to the customer, for later review, after it is first delivered. It is good practice to design the presentation so it is clear that the customer is presented with the record, and has the opportunity to review it, before signing or entering into any agreement relying on the record.
- Recipients receiving an electronic record to review or sign are often entitled to retain a copy. The methods made available to the recipient often include the option to print and/or download. In transactions involving the use of a hand-held device, delivery of a retention copy by email is also sometimes appropriate.
- A delivery method and process must be established with respect to each record being presented, based on the information contained or provided in the record. Presentation of a record during a real-time transaction may be, as appropriate, in a scroll box, pop-up or child window, or behind a clearly-labeled hyperlink. Delivery of a record via email or emailed notice should be in a common format that is easily readable with freely available software, such as PDF document.

If a Call to Action, such as a click-through button, appears in connection with a record, the Call to Action should generally appear below or to the right of the related record or records. The Call to Action generally should not appear above or to the left of the related record or records. Determine whether the recipient has a right to retain a copy of the record being delivered. If so, identify the retention method that will be used and how the recipient will be informed that the retention option is available.

Financial Advisor Authentication

When an event occurs, such as establishment of an account or transaction by or with a broker's assistance, certain governing rules must be applied. Under Financial Industry Regulatory Authority (FINRA) Rule NASD 2310, before recommending a customer purchase, sell, or exchange any security, a broker must make a suitability determination. Accordingly, because the broker has direct contact with the customer in making the suitability determination, the broker should also ensure that the customer and investment are legitimate.

Broker/dealers must adhere to "know your customer" guidelines and "customer identity program" requirements for any accounts they open. The SEC and its regulatory body, FINRA, review that adherence. FINRA Rule 4512(a)(1)(D) requires the signature of the firm's partner, officer or manager to denote that the account has been accepted in accordance with the firm's policies and procedures for acceptance of accounts. FINRA staff interpretation have approved the use of electronic signatures for qualified principal approval of new accounts or applications provided the following safeguards are in place:

- The system will allow FINRA examining staff immediate access to required records and will contain appropriate indexing and cross-referencing capabilities to assure access to all relevant documents and records. It will also ensure retention of the records and documents in accord with the FINRA and SEC's record retention requirements and rules
- The system will permit examining staff to download documents, records and information and permit printing these documents in hard copy
- The system will provide for adequate security and restriction of access to authorized employees and principals only. Company-wide user profiles should be created with previously approved authority to conduct reviews and approvals. Passwords should be changed periodically and be safeguarded against unauthorized use
- The system will be maintained in compliance with written policies and procedures of the firm
- The firm will conduct periodic reviews of the policies, procedures and operations to assure that the system operates as designed and documented and in accordance with FINRA/SEC requirements

Record Retention

It is important to recognize that with e-signatures there is no "original," as that term is used in record retention. Electronic Records will be moved or copied from one physical location to another on a routine basis. Ultimately what is seen on a display screen is not the Record itself, but a graphic display image based on instructions that are a combination of the Record and software interpreting the Record.

As a general matter, in order to ensure that electronic evidence will be admissible, a Record Holder will need to be prepared to demonstrate that the Electronic Record being offered into evidence accurately displays the relevant information from the Record created in the original Transaction. The key to admitting an Electronic Record, or a printout of the Record, is evidence of data integrity and accuracy. To date, the few court decisions focusing on the introduction of Electronic Records have emphasized the systemic protections—division of labor, complexity of backup systems, activity logs, and security of copies stored offsite to verify content—that make it difficult to counterfeit or alter a Record without leaving a discoverable trail.

As part of record retention, it will be important to make copies of generic screen shots and process flows for each material iteration of any process created for delivering electronic records and/or obtaining electronic signatures. That information must be maintained for reference for a minimum of six years. Enforcement of electronic signatures will depend, in part, on the effectiveness of the delivery and signing process.

The network will protect the processing and storage environment during the creation of electronic records and must protect the integrity of the stored records and the data contained in those records.

Electronically signed records must contain all of the information necessary to reproduce the entire electronic record and all associated signatures in a form that permits the person viewing or printing the entire electronic record to verify:

- The contents of the electronic record
- The method used to sign the electronic record, if applicable and
- The person or persons signing the electronic record

More information about these guidelines may be found through the SEC and FINRA. These electronic signature guidelines apply to the services offered by Docupace Technologies, LLC. The Docupace STP Network© e-signature solution exceeds the federal ESIGN Act, FINRA Rules and SEC requirements by utilizing electronic signature pads or remote signing through multi-factor authentication processes. For more information about Docupace STP Network©, visit http://www.docupace.com/.


Docupace
TECHNOLOGIES