K6 Partners
innovate with confidence

CURSIVE IN THE CLOUD

The Case for Handwriting Capture in SaaS eSignature Deployments

BY KEN MOYLE

WHITE PAPER

While online signature companies have distanced themselves from non-cloud solutions in the past, the combination of pen technology and SaaS signing may be the key to a complete electronic signature solution.

EXECUTIVE SUMMARY

Electronic signatures have been widely adopted and are easy to use. The success is largely driven by cloud providers who offer remote signature solutions and easy deployment. But the low-friction, cloud-based model suffers from limits on the types of transactions that can be confidently performed online. In particular, "click-to-sign" tools tend to become more complicated and less reliable for higher value transactions or those that require the physical presence of the parties.

Meanwhile, physical handwriting continues to enjoy both ease of use for signers and perceived legitimacy by relying parties. Recent enhancements to pen technology have resulted in electronic records that capture biometric artifacts as well as transaction data, creating opportunities to fill usability and compliance gaps that online signing alone has been unable to address.

While online signature companies have eschewed hardware-dependent solutions in the past, the combination of pen technology and SaaS signing may be the key to a complete electronic signature solution.

TABLE OF CONTENTS

THE ONLINE SIGNING REVOLUTION

Electronic signatures have become ubiquitous across the planet, as consumer demand and corporate productivity gains have driven the need to automate traditional paper-based processes. More recently, cloud-based deployment of digital signature solutions has gained widespread acceptance due to lower implementation costs and availability of low-cost cloud storage. Cloud-based deployments dominate the global market in terms of revenue, and are expected to maintain this trend into the foreseeable future.[1]

The legal basis for eSignatures in the U.S. was established with the Electronic Signatures in Global and National Commerce Act (ESIGN), enacted by Congress on June 30, 2000.[2] Also, 47 states, the District of Columbia, and the U.S. Virgin Islands, have adopted laws based on the Uniform Electronic Transactions Act (UETA), a model for state statutes that was made available in 1999 by the National Conference of Commissioners on Uniform State Laws. The remaining three states (WA, IL, and NY) have their own statutes to address electronic signatures.[3]

The U.S. eSignature statutes are based on common law principles of contract and evidence, not on any agreed form of attribution or authentication. An electronic signature is defined very broadly, so that parties are not inconvenienced by rigid form requirements but can determine on their own how to execute an agreement.[4]

The initial force behind the U.S. eSignature laws was the mortgage industry, for whom the ability to deliver required written notices and collect signatures without in-person interaction drastically reduced transaction time.[5] Removing friction from the process was essential, and for early use cases such as furnishing lending disclosures, complicated identity verification was not required.

With 50% of the total eSignature market in 2016, the U.S. has enjoyed massive adoption, leaning heavily on cloud-based services such as DocuSign and Adobe Sign that enable remote parties to execute reasonably secure and verifiable transactions with user-friendly "click-to-sign" tools. The ease of implementation of SaaS based eSignature systems has also led to rapid adoption in sales, human resources, and legal departments within companies.[6]

[1] Transparency Market Research (2017). Digital Signature Market - Global Industry Analysis, Size,Share, Growth, Trends and Forecast 2017 – 2025. Retrieved from: http://www.transparencymarketresearch.com/digital-signature-market.html

[2] Electronic Signatures in Global National Commerce, 15 U.S.C. §§ 7001 et seq. (2012)

[3] See Electronic Signatures and Records Act, NY CLS State Technology Law §§ 301 et seq. (1999); Electronic Commerce Security Act, 5 ILCS 175/1-101 et seq. (1998); Washington Electronic Authentication Act, Rev. Code Wash. (ARCW) §§ 19.34.010 et seq. (1999)

[4] An electronic signature is defined as "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Definitions, 15 U.S.C. § 7006(5) (2012).

[5] (R. David Whitaker, counsel at Buckley Sandler LLP, interview, July 10, 2015)

[6] P&S Market Research (2017). Global E-Signature Market Size, Share, Development, Growth and Demand Forecast to 2023. Retrieved from: https://www.psmarketresearch.com/market-analysis/e-signature-market

Adoption challenges in key industries

But the low-friction, cloud-based eSignature model has suffered from limits on the types of transactions that can be confidently performed online.

The **home mortgage** is a prime example of this type of transaction. While the major stakeholders in the mortgage industry were the driving force behind electronic signature laws two decades ago, their goal of a 100% digital mortgage system has not come to fruition: of the nearly 10 million mortgages closed in 2016, only about 5,000 were closed electronically.[7] The home mortgage ecosystem comprises many players, most of whom rely on the authenticity of critical documents (such as legally mandated disclosures, promissory notes, mortgages and deeds) but are not involved in the origination, execution, storage or delivery of those documents. Bankers, investors, servicers, wholesale lenders and county recorders must make decisions based upon identity of the parties, authenticity of the documents, and enforceability of contractual obligations, and many are not willing to make these decisions based on the perceived risks associated with "simple" electronic signing.

Healthcare delivery services have also been slow to adopt electronic signatures and records. Despite federal legislative support for the nationwide use of electronic health records (EHR)[8] , healthcare transactions and records are confined largely to paper and transmitted by facsimile rather than online. Early concerns about compliance of email with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 led the entire industry to eschew the internet in favor of facsimile transmissions. Improvements to online security and the emergence of communication channels more secure than email have not yet convinced many in the industry to offer alternatives to paper and ink. That is not to say that the industry has not adopted technology; on-premise solutions are very common in healthcare, but manual entry of patient information and paper capture of patient and practitioner signatures are the starting points for much of the data.

Electronic transactions are also in short supply in **retail banking**, where handwritten signature cards are still common and in-branch interactions are documented on paper. Compliance with banking regulations as well as the ESIGN Act are cited as concerns, as is the relative awkwardness of using click-to-sign in an in-person context.

Insurance has also been slow to adopt electronic signatures. Mobile agents insist that online signing is technically cumbersome and provides a poor client experience. Insurance providers have concerns about agent misuse of click-to-sign technology at the point of sale. Taken together, many of the barriers to adoption of electronic signatures are tied to the limitations of a 100% hosted solution.

[7] Michael Lewis. (2017, September 7). First Paperless Mortgage Closed Using Webcam Notarization. Notary Bulletin.Retrieved from: https://www.nationalnotary.org/notary-bulletin/blog/2017/09/first-paperless-mortgage-closed-using-webcam-notarization

[8] Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 42 U.S.C. §§ 300jj et seq. (2012) and 42 U.S.C. §§ 17921 et seq. (2012)

LIMITATIONS OF CLICK-TO-SIGN

While the market for simpler digital transactions remains robust, the opportunity to extend the advantages of digitization to higher tier transactions in the cloud remains limited.[9] Complex, multi-party, high risk, or in-person transactions that rely heavily on identity and compliance have lagged. The limitations arise from heavier dependencies on 1) assurance of signer identity, 2) physical presence of the parties or witnesses, and 3) acceptance of the record by third parties, including regulators.

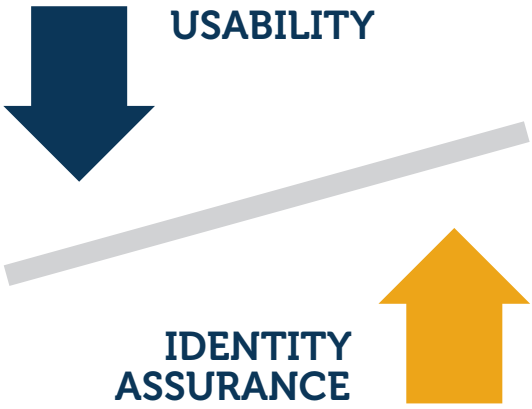
The authentication problem

Online identity has vexed the ecommerce community for two decades. The earliest resistance to internet transactions stemmed from the question: "How do I know it's really you?" Tying an individual's identity to the act of signing, and tying that result to the document purported to have been signed, is called attribution. Along with record integrity (i.e. the security applied to the electronic record to ensure its authenticity), attribution is a key component of a valid and enforceable signature. Without adequate means of attribution, the electronic signature has little value.

No standard for online attribution

American electronic commerce laws did virtually nothing to address this problem; rather they opted for allowing the parties to determine for themselves the best means for determining attribution. For simple, bilateral agreements or electronic delivery, this was arguably the right choice. But in more complex transactions, or in situations where there are many parties and non-parties relying on the authenticity of the document and its components, the lack of standards has weakened the prospects for going digital.

Attempts to address this issue were advanced in Europe and other civil law countries. While North America was building private sector e-commerce platforms to support low-risk, low value transactions in the 1990's, Europe instead worked on an electronic authentication model that focused on minimizing online risk in order to support a "digital agenda" for online delivery of government services. Rather than leaving attribution and authentication decisions up to the parties, the Europeans focused their eSignature regime almost exclusively on identity. Governments needed to rely on electronic documents presented to them by citizens of other countries, or by other countries' governments. Authenticity and reliability were paramount to eliminate unnecessary risk. Not only was identity a component of an electronic signature, it was synonymous with an electronic signature. After passage of the "Directive on a community framework for electronic signatures" in 1999, or E-Signature Directive,[10] European standards bodies spent years defining technology and process requirements to support legal certainty for digital documents.



[9] Ken Moyle (2015, May 20). Are We Stuck in E-Adolescence? K6 Blog. Retrieved from: http://www.k6blog.com/2015/05/are-we-stuck-in-e-adolescence

[10] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Retrieved from: http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31999L0093

The results of these experiments were disappointing. The high-assurance eSignature models—such as those found in Europe, Latin America, and many other non-Common Law countries—have imposed a very high threshold for compliance and a technical barrier to simple transactions that inhibits practical adoption.

In Germany, where digital signing technology was designed into the national identity card, few users had activated the signing functionality seven years after it was made available.[11] And deploying the European signature regime anywhere in the cloud to enable remote transactions was not even considered possible. At the same time, the more accessible U.S. model garnered a dubious reputation in Europe, Latin America and Asia as being too lightweight to be considered legally enforceable.[12]

To offset the lack of a universal authentication mechanism, authentication standards have emerged in key industries and government. The National Institute of Standards and Technology, or NIST, has been promulgating identity guidelines for many years.[13] The Federal Financial Institutions Examination Council, or FFIEC, has since 2005 published guidance for the financial services industry.[14] These and other guidelines have aligned themselves with the concept of multifactor authentication[15] to address the problem of online identification of parties.

The "factors" considered are:

- **SOMETHING THE USER KNOWS** (e.g., password, PIN);
- **SOMETHING THE USER HAS** (e.g., ATM card, smart card);
- **SOMETHING THE USER IS** (e.g., biometric characteristic, such as a fingerprint).[16]

SaaS eSignature solutions have developed effective ways of obtaining the first of these. The challenge for click-to-sign has been how to authenticate a user with an additional factor.

Presumptions about handwriting

Industry reluctance to adopt electronic signatures often stems from the perception that a true signature must create a biometric link between the signer and the document. Case law throughout the common law world has demonstrated that, despite what statutes like ESIGN and UETA say, the value of a signature is often determined by whether it is physically affixed by hand to a document.[17]

[11] Sorge, C. (2014). The German Electronic Identity Card: Lessons Learned. Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services. IGI Global. Retrieved from: https://books.google.com/books?id=hSgdBgAAQBAJ

[12] See e.g. German Digital Signature Law (SigG) (1997). Translation at:http://www.kuner.com/data/sig/digsig4.htm

[13] Grassi , P. A., Garcia, M. E., & Fenton, J. L. (2017). SP 800-63-3 - Digital Identity Guidelines. NIST. https://doi.org/10.6028/NIST.SP.800-63-3

[14] (FRS SR, Letter 05-19, October 13, 2005). (FDIC, Financial Institution Letter 103-2005, October 12, 2005) (NCUA, Letter to Credit Unions 05-CU-18, November 2005) (OCC, Bulletin 2005-35, October 2005) (OTS, CEO Memorandum 228, October 12, 2005)

[15] See Grassi, Garcia, & Fenton (2017), p.18; FFIEC (2005) Authentication in an Internet Banking Environment. October 12, 2005, p.3. Retrieved from: https://www.ffiec.gov/pdf/authentication_guidance.pdf

[16] See FFIEC (2005), p.3.

[17] See e.g. Neuson v. Macy's Dept. Stores, Inc., 249 P.3d 1054 (Wn. App. 2011), Ruiz v. Moss Brothers Auto Group, Inc., 232 Cal. App. 4th 836(Cal. App. 4th 2015), Ni v. Slocum 196 Cal. App. 4th 1636 (Cal. App. 4th 2011)

This is not merely a perception problem. Handwriting has long been an essential element in many internal control frameworks to combat fraud. Signatures serve as detective controls, empowering parties to defeat attempts to repudiate agreements that they have signed in the past. And they are used broadly in the financial services arena as preventive controls, to compare signatures on drafts or transfer instructions against known signature samples. In fact, "signature cards" are referred to in banking regulations and are presumed to be necessary to comply with FDIC rules.[18]

In support of its own specific requirements for accepting electronic signatures, the Federal Aviation Administration says: "To be considered valid, an electronic signature must provide equivalent qualities and attributes to those that are identified with a handwritten signature. A handwritten signature is universally accepted because it typically contains qualities and attributes that are unique and can easily be identified as belonging to the individual signatory."[19]

AN ELECTRONIC SIGNATURE REQUIRES A FORM OF AUTHENTICATION; A HANDWRITTEN SIGNATURE IS FORM OF AUTHENTICATION.

The fact is that, while electronic signatures must normally be backed up by some form of authentication, handwritten signatures often ***are*** a form of authentication. This is doubly true in civil law countries, where a handwritten signature alone carries a presumption of authenticity, a status that cannot be met electronically without rigorous third-party identity verification.[20]

The in-person signing experience

Point of sale interactions and witness requirements have received very little attention from cloud signature vendors, in part because such transactions do not take advantage of non-contemporaneous signings or non-co-located parties, which are the two more obvious benefits of signing electronically. Further, remote transactions sometimes require parties to be offline and unable to access cloud services during key parts of the exchange.

Opening an account at a retail banking branch, applying for insurance through a local agent, or filling out an admission form at a hospital are still routinely done with pen and paper. Bankers, agents, support staff and medical practitioners themselves also conduct their daily business with paper documents and handwritten signatures.

[18] See 12 C.F.R. § 330.9(c)(ii)

[19] FAA Order No. 8900.1, Volume 3, Chapter 31, Section 2 (2016). http://fsims.faa.gov/wdocs/8900.1/v03%20tech%20admin/chapter%2031/03_031_002.htm

[20] Christopher Kuner & Anja Miedbrodt (1999). Written Signature Requirements and ElectronicAuthentication: A Comparative Perspective. Retrieved from http://www.kuner.com/data/articles/signature_perspective.html.

As inconvenient as "paperwork" can be to consumer and provider alike, signing such documents on a computer screen in the presence of the parties has not emerged as a high priority for either. User experience concerns are partly responsible for this. Because electronic signature solutions have focused heavily on supporting remote party transactions, they tend to impose authentication and signing structures that do not fit comfortably into a face-to-face exchange.

In the case of an in-branch banking transaction, the simple act of signing a document can become more complicated and awkward by introducing an electronic interface – such as a computer monitor or a mouse – into the process.[21] Early attempts to capture customer data and signatures in the branch have involved sharing a computer screen with the signatories and using a key pad or mouse to "sign" documents, rather than the more familiar and intimate act of applying a handwritten signature. Because the hardware is shared, signatories must be individually authenticated as part of the process, which puts the parties in the awkward situation of having to convince the computer they are who they purport to be. When faced with this so-called "swivel signing" ceremony, consumers frequently express frustration and ask why they cannot simply sign with a pen.

ABOUT THE AUTHOR

Ken Moyle is President of K6 Partners LLC. A legal and policy veteran in the high tech community, Mr. Moyle has held in-house leadership positions at start-ups, "unicorns" and publicly traded enterprises, most recently as chief legal officer of DocuSign, Inc. Mr. Moyle is an internationally recognized expert in digital transactions, e-signature, and legal technologies. He is a graduate of University of Washington School of Law.

Life insurance transactions frequently take place in homes, some of which can be without reliable wifi or local cellular data coverage. Cloud-based signing relies on a live connection to the internet in order to provide real-time signature capture and a verifiable audit trail. The lack of a reliable way to capture a verifiable electronic signature in this scenario has resulted in falling back to traditional handwritten signatures on paper documents.

From the perspective of SaaS technology providers in the U.S., in-person electronic signing has posed significant challenges. The cost savings and convenience that attend the conversion from paper to electronic are harder to measure when the obvious benefits of remote signing are not part of the equation. Further, as cited above, there is a mismatch between the authentication methods that work well for SaaS implementations and the needs of the parties who are sitting face-to-face. Finally, the real-time capture of signature metadata by a third-party cloud service, when the signing is taking place on-premise and could easily be captured by a secure service behind the firewall, is of limited value.

Acceptance and Compliance

Throughout the two decades since the enactment of ESIGN and the E-Signature Directive, there has been resistance to electronic signatures. The Electronic Signature & Records Association has highlighted many instances of broad prohibitions or limitations on electronic transactions by governments, government sponsored private enterprises, known as GSEs, and entire industries, including insurance and home mortgage.[22]

[21] Chris Joyce (2009). Electronic Signature Capture: Signing Up for More Efficient and Compliant Healthcare Delivery. Bottomline Technologies, Inc. Received from: http://archive.bottomline.com/collateral/ healthcare_solutions/Electronic%20Signature%20Capture%20Whitepaper.pdf

[22] Electronic Signature & Records Association. Retrieved from: http://www.esignrecords.org

Over the years, much of the resistance has taken the form of quasi-legal arguments that have merely masked the discomfort with change or misunderstanding of the technology and how it was to be used.

In a study on how organizations are moving to be less paper intensive in their processes, more than 50% of respondents said that they print documents solely for the reason of adding a signature.[23] In a 2016 whitepaper, the Association for Information and Image Management (AIIM) found that "there is a lingering sense that a 'wet ink' signature, one that is handwritten on a physical piece of paper at times with the use of colored ink, like blue, is more trustworthy and valid than an eSignature."[24]

This has had a chilling effect on adoption by those who find themselves needing their electronically executed documents accepted by downstream trading partners or agencies that, for whatever reason, do not accept them.[25] In fact, the same organizations promulgating digital transactions themselves will often adopt policies against accepting or acknowledging such transactions from others.[26]

"THERE IS A LINGERING SENSE THAT A 'WET INK' SIGNATURE IS MORE TRUSTWORTHY AND VALID THAN AN ESIGNATURE."

Nevertheless, some of the obstacles to adoption ofelectronic signatures are very real. Whether by law orby technological barrier, some types of transactions donot fit into the click-to-sign paradigm:

- Credit card transactions at POS
- Bank account signature cards
- Medicare Part B providers and drug prescriptions
- Some powers of attorney
- Notarial acts
- Wills and trusts
- Deeds
- Promissory notes
- Patient consents to treatment
- Authorizing physician credentials
- Bills of lading
- Life insurance applications
- Mortgage origination
- In-person delivery of ESIGN disclosures

[23] AIIM White Paper (2016). E-Signatures in Europe: Understanding the legal requirements for proof of intent. Association for Information and Image Management. Retrieved from: http://info.aiim.org/e-signatures-in-europe-understanding-the-legal-requirements-for-proof-of-intent

[24] Id.

[25] Leslie Rouda Smith (2013, March 25). E-Sign on the Dotted Line. Voices of Real Estate. Retrieved from: http://voicesofrealestate.blogs.realtor.org/2013/03/25/e-sign/. Hugh Fitzpatrick (2015, February 22). Showing little sign of progress on e-closings. Boston Globe. Retrieved from: https://www.bostonglobe.com/business/2015/02/22/why-don-more-lenders-accept-electronic-signatures/2gShmHz2xopN0XYtMxTBeL/story.html

[26] Department of Health and Human Services (2017). Medicare Signature Requirements Fact Sheet. Retrieved from: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Signature_Requirements_Fact_Sheet_ICN905364.pdf

This is not to say that cloud-based click-to-sign solutions cannot be used in these situations, but the manner of signing and the SaaS back-end make it difficult to execute these types of transactions on a large scale.

In fact, in some cases legislation imposes a greater compliance burden on digital transactions than on handwritten signatures. For example, a California appeals court held that the UETA requires a specific and documented (provable) act of intent to sign a document for the signature to be valid.[27] Because handwritten signatures are not prescribed in law and do not have a common law definition, they are not subject to the same scrutiny.

Courts and the legal profession have also had difficulty adapting to changes in technology. A large body of forensic research has accumulated over many years, dedicated to analyzing handwriting and detecting forgery.[28] Litigators and judges alike have developed practices around admitting signatures into evidence and making arguments as to their validity. Handwriting experts are plentiful and their methods well documented. These practices do not apply to click-to-sign signatures; indeed, research has shown that even signing by hand with a mouse may render a signature forensically unreliable.[29] And while the means of authenticating an electronic signature in court are varied and robust, they are different enough from the commonly accepted notions of signature verification to cause concern and slow adoption.

HOW DIGITAL PEN TECHNOLOGY CAN HELP

Physical handwriting continues to enjoy both ease of use for the signer and perceived legitimacy by relying parties. Throughout the era of technological exploration into electronic identity and high-assurance digital signing, the old-fashioned handwritten signature still seems immune to second-guessing. A handwritten signature benefits from historical advantages that have been culturally adapted and codified in law, and in some cases, offers an escape route for burdensome technical requirements often placed on electronic signatures.

[27] JBB Investment Partners Ltd. et al. v. Thomas Fair et al., 232 Cal. App. 4th 974 (Cal. App. 4th 2014). See also Tim Banks (2017, April 3) A Cautionary Tale Regarding Consent and In-Store Tablets. JDSUPRA. Retrieved from: http://www.jdsupra.com/legalnews/a-cautionary-tale-regarding-consent-and-10771/

[28] Harralson, H. H. (2016). Developments in Handwriting and Signature Identification in the Digital Age. London and New York: Routledge.

[29] Id. at page 89.

Digital pen technology captures electronically handwritten context and applies this data to digitized forms. Digital pens are not styli; they are electronically enhanced tools that are used in various industries, such as healthcare; banking & finance; IT; and telecom.

Breaking down the authentication barrier

Digital pen technology provides the ability to capture and verify signatures with simultaneous biometric data-capturing and analysis. By introducing biometrics into the multifactor authentication mix, pen technology opens up new options for transactions that mandate medium or high assurance levels.

The presumption of the authenticity of handwriting is evident in state laws and regulations throughout the U.S. The Food and Drug Administration, or FDA, provides for separate, more stringent rules for authenticating electronic signature systems that do not contain a biometric component.[30] Even digital signature rules have codified exceptions for "signature dynamics," which provide a means of meeting authentication requirements simply by using technology that can capture nuances of handwritten signatures, rather than submitting to rigorous third-party identity verification.[31]

Not coincidentally, point-of-sale digital authentication and signing devices have enjoyed high adoption in civil law jurisdictions like Europe and Latin America, because they are able to address this paradox by keeping the handwriting part and digitizing the workflow around it.

Enhanced usability for in-person transactions

That banks must "go digital" is a foregone conclusion. Marketing experts have commented that banks "must be on their high-tech toes or they risk pushing the customer into the waiting arms of another bank – or an online service such as PayPal."[32] Yet user experience designers have lamented the lack of association between the human act of signing and the click of a mouse.[33] Some studies even indicate that people feel less committed to binding terms when concluding a contract with a click instead of written signature.[34] As noted above, handwriting remains the most natural form of signature expression. Digital pen technology provides a bridge between the customary signing ceremony and the necessary collection of electronic data.

As banks continue to move away from across-the-desk interaction, technology is helping with account origination and other basic banking tasks, with the banker and customer working together over a tablet to execute the transaction.[35] Digitally captured signatures can be used for multiple purposes, including lobby sign-in and electronic account signature cards.[36]

In the healthcare arena, physicians and patients are warming up to digital pens and tablets that emulate the pen and paper experience.[37]

[30] 21 C.F.R. 11.200.

[31] See e.g. List of Acceptable Technologies, 2 Cal. Code Regs. § 22003(b)

[32] Meredith Dean (2015, June 5). Marketing to millennials in-branch and out. BAI Banking Strategies. Retrieved from: https://www.bai.org/banking-strategies/article-detail/marketing-to-millennials-in-branch-and-out.

[33] Jamie Myrold (2016, April 2). Signatures and Ceremony: Adding Emotion to Electronic Signatures. Uxdesign.cc.
Retrieved from: https://uxdesign.cc/signatures-and-ceremony-adding-emotion-to-electronic-signatures-9b49513dc5e

[34] See e.g. Chou, E. Y. (2016). What's in a name? The toll eSignatures take on individual honesty. Journal of Experimental Social Psychology, 61, 84-95. https://doi.org/10.1016/j.jesp.2015.07.010

[35] Penny Crosman (2013, January 23). Chase, RBC Sign Off on E-Signatures. American Banker. Retrieved from: https://www.americanbanker.com/news/chase-r-bc-sign-off-on-eSignatures

[36] Penny Crosman (2013, April 10). U.S. Bank Broadens Use of E-Signatures to Loans. American Banker. Retrieved from: https://www.americanbanker.com/news/us-bank-broadens-use-of-eSignatures-to-loans

[37] Marc Paskett (2014). Case Study: Columbia Valley Community Health. Access. Retrieved from: https://www.accessefm.com/case-studies/columbia-valley-community-health

Compliance and acceptance by third parties

Pen technology can preserve forensic information of signatures with pressure and dynamics, providing a high degree of personalization and security, as every signature will be unique yet identifiable. Digital pen signing can also provide real-time preventive and detective controls.

In Europe, many transactions are already being confirmed by biometric signature technology. In the U.S., pen interfaces are now getting traction with financial institutions that are transforming the in-branch banking experience, focusing on higher-value, high-touch transactions with higher-value customers.

By nature, a signature is unique, making it automatically in compliance with key provisions of digital signature laws. And unlike a mouse click, a pen-drawn signature is given deliberately with the presumption of intent.

Government acceptance of digital pen signatures is well documented. Santa Clara, CA, was reportedly the first county in the nation to accept electronic voting registrations.[38] Denver Elections Division launched a pilot program in 2015 that allowed collection of registered voter signatures on ballot petitions. Because the method of collection involved pen technology, signatures could be compared to those of registered voters on file with the Division. The rejection rate for the electronically captured signatures was 3%, compared to over 30% for paper petitions.[39]

Banks that abandon paper sign-in sheets and embrace pen technology can collect and analyze data on a bank-wide basis to better identify individuals that may have tried to perpetrate frauds at other locations.[40]

The introduction of signature tablets in healthcare has demonstrated how adoption can be enhanced by handwriting tools. HIPAA compliant data capture and positive patient feedback are common.[41]

[38] Ken McLaughlin (2010, May 14). Santa Clara County accepts nation's first electronic voting registrations. The Mercury News. Retrieved from: http://www.mercurynews.com/2010/05/14/santa-clara-county-accepts-nations-first-electronic-voting-registrations/

[39] Amber Reynolds (2015). Connecting Customers to Data: eSign – Electronic Signature Image Gathering Network. Office of the Clerk and Recorder. Retrieved from: https://electioncenter.org/publications/2015PPP/Denver_CO-eSign.pdf

[40] W. Michael Scott (2014). Catching Fraud at the Branch Level. FMSI. http://www.fmsi.com/catching-fraud-at-the-branch-levelblets. JDSUPRA. Retrieved from: http://www.jdsupra.com/legalnews/a-cautionary-tale-regarding-consent-and-10771/

[41] See supra note 37, Mark Paskett (2014).

WHY DIGITAL PEN TECHNOLOGY HAS NOT BEEN USED WITH CLOUD ESIGNATURE SOLUTIONS

Immature technologies. As recently as 2008, studies showed that the technical limitations of pen computing created a drag on use experience, with one reporting that "pen only input is difficult to achieve with a standard operating system because the pen is appreciably overloaded."[42]

The electronic signature capture systems used by most retailers have not historically captured signatures that allow for forensic analysis,[43] but such systems are not built for such analysis. In the healthcare space, it has been a common notion that "technology is good enough to record the information and to improve care, but not good enough to make daily work easy for clinicians."[44] Misperceptions about available technology abound.

In-person transactions are not top priority for SaaS vendors. SaaS applications need to be connected to the cloud, and SaaS eSignature providers rely on connectivity to capture, record and retain important data in real time. Further, it is fundamental to the concept of a remote party transaction that participants will be connected to the internet. In-person transactions, however, are commonly conducted without internet connections, and often take place in locations where a secure network connection is not available. These obstacles have led SaaS eSignature providers to deprioritize in-person use cases.

Digital pen providers are rarely identified as market participants in the electronic signature space, or its new moniker, Digital Transaction Management. The electronic signature market—as reported by analysts Forrester, Aragon, and Gartner—comprises cloud software vendors almost

[42] Plimmer, B. (2008). Experiences with digital pen, keyboard and mouse usability. Journal on Multimodal User Interfaces, 2(1), 13-23. doi:2. 13-23. 10.1007/s12193-008-0002-4

[43] David R. Wheeler (2012, January 25). Signing Off: The Slow Death of the Signature in a PIN-Code World. The Atlantic. Retrieved from: https://www.theatlantic.com/technology/archive/2012/01/signing-off-the-slow-death-of-the-Signature-in-a-pin-code-world/251934/

[44] Dr. Suzanne Koven (2014, February 24). In Practice: Doctors, Patients and computer screens. The Boston Globe. Retrieved from: https://www.bostonglobe.com/lifestyle/health-wellness/2014/02/24/practice-doctors-patients-and-computer-screens/JMMYaCDtf3mnuQZGfkMVyL/story.html

exclusively, listing pen technology as a special use case.[45] Even a March2017 report on digital signatures focused on the growth of cloud deployments of signatures.[46]

Cloud services have overcome initial resistance by declaring superiority over behind-the-firewall IT installations. So much so that many SaaS vendors have taken a purist view of service delivery. SaaS eSignature vendors have historically been reluctant to adopt or propose on-premise solutions partly because hardware is anathema to their concept of "the Cloud," where everything is delivered and managed remotely. To preserve the SaaS delivery model, steps are often taken to avoid physical interaction with local devices wherever possible, even where such interaction is a natural outcome of the transaction, such as writing one's name.

WHY IT'S TIME TO TAKE ANOTHER LOOK AT PEN TECHNOLOGY

As technology advances and consumer demands change, it is incumbent upon users and providers of eSignature solutions to evaluate new options and enhancements. Pen technology is no exception.

The need has become obvious

The "low hanging fruit" of SaaS eSignature technology providers has been the remote party transaction. Eliminating the costs and time loss associated with such transactions has had clear and measurable hard-dollar ROI. However, with the automation of more back-office processes and the sophistication with which transaction data is collected and stored, the benefits of interacting with documents electronically have increased far beyond simple cost savings. Electronic capture of party data is essential, regardless of whether it is captured remotely or at the point of sale.

It is now clear that different tools are needed to address specific use cases and security requirements, including the use of hardware and software solutions for in-person transactions. Such tools by their nature are not 100% SaaS – they involve the use of physical technology to enhance the customer experience and improve compliance.

[45] Penny Crosman (2013, April 10). U.S. Bank Broadens Use of E-Signatures to Loans. American Banker. Retrieved from: https://www.americanbanker.com/news/us-bank-broadens-use-of-eSignatures-to-loans

[46] Allied Market Research (2017). Digital Signature Market by Component (Hardware, Software, Services), Deployment Type (On-premises, Cloud-based), Industry Vertical (BFSI, Education, Human Resource, IT & Telecommunication, Government, Healthcare & Life Science, Real Estate) - Global Opportunity Analysis and Industry Forecast, 2014 - 2022. Retrieved from: https://www.alliedmarketresearch.com/digital-signature-market

Pen-based technology has evolved

The technological advancement and new features of digital pens, and their increasing use for reducing deception are driving the growth of the global market.[47]

Active Pen

For signatures, pen technology has until recently been only associated with so-called "signing pads," those boxy terminals one encounters at a grocery store or at a bank teller station. The limits of the technology precluded efforts to go beyond mere imitation of a paper signing experience.

The active pen industry landscape has changed dramatically in just the past 2 years, and technology has advanced to allow for additional control and security. The number of companies actively working on active pen technology has increased from 60 companies in 2014 to over 100 companies in 2016. Apple engineered the Apple Pencil to work with its iPad tablets. Microsoft acquired N-trig's pen technology in 2015 for its Surface laptops. In 2014, Wacom expanded the lineup of digital pen technologies and announced the development of Active ES pen type. Many active pen companies have raised capital through Kickstarter. Over 10,000 people have backed those pen projects.[48]

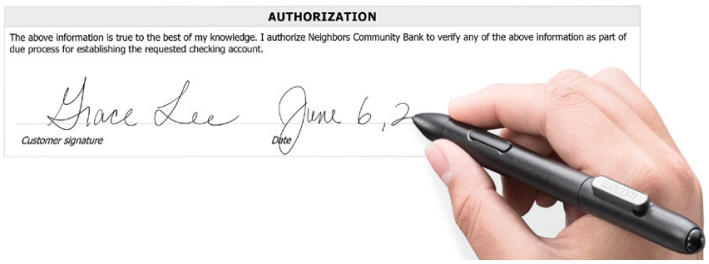
With the release of the Samsung Galaxy Note 8 in 2017, the S Pen offered a new user experience to verify a person's identity using eSignature solutions combined with biometric authentication.[49]

Advances in pen technology are providing forensic analysts with an opportunity to analyze the digitally produced data of signatures in new ways. "Temporal, dynamic data related to the speed and pressure of the signature can now be captured and quantified, data that can only be estimated by examiners when examining the static trace from pen and ink signatures."[50]

Signature Display

The different tablet devices available on the market can impact the handwriting signal significantly. Commercially available tablets manufactured by Wacom Co., Ltd., and used extensively in handwriting research, rely on electromagnetic induction to transmit and receive information to and from the active pen. These signals help establish the position of the pen on the tablet.

Tablets can now receive signal information from the pen without the pen touching the tablet. This helps identify



[47] See supra note 6, P&S Market Research (2016).

[48] Jennifer Colegrove, PhD (2016, March 22). Active Pen market will reach $6.1 billion by 2021. Touch Display Research. Retrieved from: http://touchdisplayresearch.com/?page_id=2576

[49] Wacom Technology Solution Business Unit (2017, September 4). Wacom's Digital Pen Technology Introduces Refined "S Pen" for the New Samsung Galaxy Note8, Offering a More Productive, Creative and Personal Digital Pen Experience for Smartphone Users. Wacom. Retrieved from: http://www.wacom.com/en-ar/about-wacom/news-and-events/2017/1257

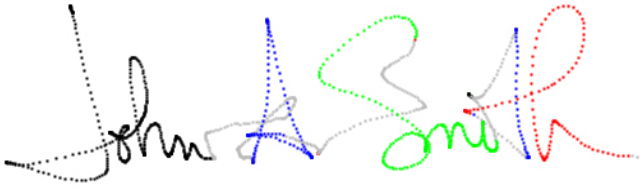
[50] See supra note 28, Harralson (2016).

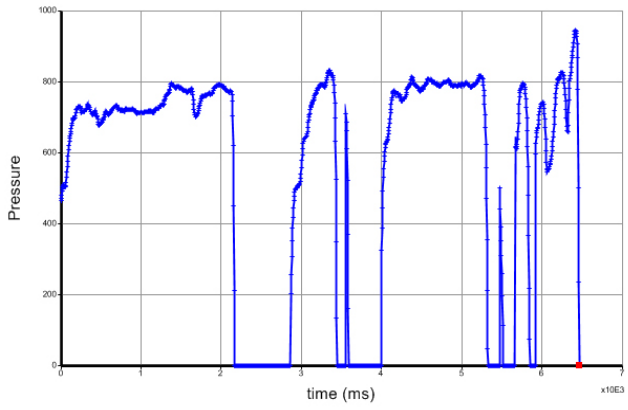
the location of the pen tip above the tablet (known as pen position), pen tilt, and x and y positions on the tablet, and time and pressure data.

Air strokes, the motion of the pen in the air when it is breaking between letters or words and creates a pen lift, can be analyzed from pen position. This accommodates the capture of some of the unique handwriting attributes that can be used to prevent fraud and unauthorized access, or to inform various forensic detection methods.

On most of today's digital tablet surfaces with an active display, the user can see the signature or drawing as it is produced on the surface of the tablet in real time. The writing appearing on the active display is referred to as "digital ink." Digital ink helps to create a more natural signing environment where the signer can see the signature being written in real time on the display.

Paired with active pens, signature displays can record signatures with biometric information plus computer/





Index	Stroke	Btn	X	Y	T	P
1235	12	1	8456	2795	31491	766
1236	12	1	8436	2913	31496	780
1237	12	1	8422	3033	31501	789
1238	12	1	8416	3155	31506	795
1239	12	1	8415	3277	31511	803
1240	12	1	8419	3400	31516	807
1241	12	1	8426	3517	31521	810
1242	12	1	8435	3630	31526	805
1243	12	1	8445	3733	31531	808
1244	12	1	8455	3826	31536	809

pad context information.[51] Users may define capture settings, such as security settings and several options for image output, and also report the details of an existing signature (who, when, why, capture and security details).

Of critical importance is the ability of these displays to capture and analyze signature data offline, which provides electronic signature options where there is no real-time connection to the cloud.

Signature verification software

Signature verification software analyzes both an exact (static) image of the signature as well as the signature's biometric (dynamic) characteristics captured on a signature display. This data assists in automating the process of authenticating users or documents.

Modern dynamic signature verification, or DSV, uses biometric information to determine the level of similarity between signatures.[52] DSV software can compare very specific aspects of the shape of different parts of the signature, called geometries. No two signatures will be identical, but many features can be compared and given a score in the verification process. The features include the pen stroke sequence, direction, speed, pressure, among others.

A key advantage of a DSV arrangement is that signature data can be used as a preventive control, as well as an authentication factor in addition to a password or hard token.

[51] Id. at 87.

[52] Id. at 80.

HANDWRITING CAPTURE SHOULD BE PART OF A DIGITAL STRATEGY

To date, worldwide eSignature adoption has been driven by SaaS providers offering rapid deployment, measurable ROI and high customer satisfaction. However, SaaS implementations have in some ways become victims of their own success, leaving large gaps in their market due to their focus on remote transactions and hardware-agnostic, cloud-only delivery of eSignature services.

It is becoming clear that a combination of pen technology and SaaS signing may be the key to a complete electronic signature solution. Advances in pen technology have resulted in electronic records that capture biometric artifacts as well as transaction data, creating opportunities to fill usability and compliance gaps that online signing alone has been unable to address.

Elimination of handwriting need not be the goal of digital transformation, nor should the appropriate use of on-premise tools be viewed as an admission that the SaaS model is somehow flawed. Physical handwriting continues to enjoy both ease of use for signers and perceived legitimacy by relying parties. Pen technology offers a natural and less complicated means of interacting at the point of sale, while capturing data that can be used effectively in a cloud-based deployment.

Cloud vendors and eSignature users should be open to the idea that even cloud-first applications will need to occasionally "touch ground" in order to provide a complete solution.