Legality of Electronic Signatures
January 2015
Electronic Signatures are Everywhere, and Come in Many Forms

An electronic signature is 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.”

- 15 USC 7006 (ESIGN Act)
Legal Foundation for Electronic Contracts and Signatures

Common Law (contract formation based on offer, acceptance, consideration)

Legislation

- United States (state and federal)
  - UETA
  - ESIGN
- International
  - European Directive 1999/93/EC
  - Electronic Transactions Act (UK)
  - Uniform Electronic Commerce Act (Canada)
  - 1996 UNCITRAL Model Law on Electronic Commerce
  - Many more (at least 40 countries have laws enabling electronic signatures)
Uniform Electronic Transactions Act (UETA)

- Drafted by Uniform Law Commission (responsible for UCC) in 1999
- Response to states adopting inconsistent laws to govern electronic records and agreements.
- Overlay statute that amends state laws or rules that require “writing” or “signature”
- Adopted quickly, but California adopted with a number of exceptions
- Now adopted in 47 states + DC, Puerto Rico, Virgin Islands
  - New York, Washington, and Illinois also have laws permitting electronic signature that aren’t based on UETA
Electronic Signatures in Global and National Commerce Act (ESIGN)

- Passed by Congress in 2000
- Federal version of UETA
- Consumer protections
  - If the consumer has a right to receive information on paper, it may be provided electronically only if consumer disclosure requirements are met
  - Improper consumer disclosure does not render the underlying contract invalid
  - Consumer notice requirements mirrored in some states’ implementation of UETA
- Preemption of nonconforming state laws
  - Laws conforming to the model UETA are not preempted
General Rule of Validity

Central concept of UETA, ESIGN, and other state laws:

A signature, contract, or other record related to any transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.

No specific technology or process must be used, and ESIGN specifically preempts any state law that would require or give greater legal status to a particular technology.

Permissive rather than proscriptive – no one is required to do business electronically, but if the parties choose to do so it may not be denied validity on those grounds.
International Landscape

Most Common law jurisdictions, including the US, Canada, the UK, and Australia, follow a “minimalist” model, where electronic signatures are the legal equivalent of a handwritten signature.

Most Civil Law countries (including most of Europe and Latin America) follow a “two tier” approach to electronic signature, modeled on the 1996 UNCITRAL Model law on Electronic Commerce.

- “Simple” electronic signature is admissible as evidence, and generally sufficient for commercial transactions
- “Qualified Electronic Signature” may have extra legal weight (such as a presumption of authenticity), or may be required for certain purposes, such as submitting documents to government agencies.
  - QES must use specific cryptographic technology called Public Key Infrastructure (PKI)
  - The PKI process involves a digital certificate, which must be issued by a Certificate Authority that is approved by the government (or issued by the government itself)
Practical Issues using Electronic Signature

Legal Sufficiency vs. Enforceability

- UETA and ESIGN answer the question “is it a signature?”
- They do not answer the question “is it your signature?”
  - Attribution will be a matter of fact, just as it is with a wet signature

Evidence

- Admissible under FRE, but subject to the same rules
- Electronic process often provides more evidence than a paper process
  - Time and Date stamp, IP address, etc.
Considerations in Implementing Electronic Signature

• Are my documents excluded from ESIGN and UETA?
  – Can they be electronically signed/recorded under some other rule or statute?
    – Probate law (electronic wills permitted in Ohio, little case law elsewhere)
    – Court rules
    – Portions of the UCC

• How will our process address:
  – ESIGN Consumer Consent (when it applies)
  – Notice and Delivery
  – Signature process – intent and attribution
  – Recipient’s right to retain copies
  – Document integrity and audit trails
What is holding us back?

"We need a handwritten signature for..."

- Proof in court
- ‘Important’ documents
- ‘legal’ documents

- Consumer agreements
- International agreements
- Government audits
Proving a signature in court

“Is this your signature, madam?”

If the alleged signer denies it, how do you prove it?

• Other evidence
  • Witnesses (if available)
• Handwriting experts
  • Must challenge opposing handwriting expert
What the *real* courts say
Sufficiency of Electronic Signatures and Records

Barwick v. GEICO (2011 Ark. 128)

Arkansas Supreme Court rejected argument that electronic waiver of medical benefits was not a “signed writing”, citing the plain language of the Arkansas UETA.

Electronic Signatures meet Statute of Frauds writing requirements

- *Rosenfeld v. Zerneck*, 4 Misc. 3d 193, 776 N.Y.S.2d 458 (Sup. Ct., Kings Co. 2004) (but see *Vista Developers Corp. v. VFP Realty LLC*, 17 Misc. 3d 914, 847 N.Y.S.2d 416 (Sup. Ct., Queens Co. 2007) – Signed emails could be used to prove the existence of a real estate contract.
**eCommerce: Clickwrap and Browsewrap Agreements**

**Fteja v. Facebook**

Online terms held to be **enforceable** where:

- Terms presented in hyperlink immediately below “Sign Up” button
- Sign Up process involved multiple steps

The fact that Facebook did not force Fteja to review the terms was considered irrelevant

**Jerez v. JD Closeouts**

Online terms held to be **unenforceable** where:

- Terms of Sale were not directly referenced in the order process
- Terms were presented only on the “about us” page

The court determined that the contract terms weren’t “reasonably communicated”

As a general rule, clickwrap, where the user takes some affirmative action, and has reasonable notice of the contract terms, has been enforced.

Browsewrap, where the terms are available, but no action is required to accept or acknowledge them, are much less likely to be enforced.
**Attribution**

**Zulkiewski v. General American Life**

Under UETA (Michigan), an electronic signature may be attributed to a person by “any reasonable means”. Here, General American used a combination of email and personal information.

Idle conjecture about impersonation is not enough to overcome reasonable facts supporting attribution.

**Record Integrity**

**Adams v. Quicksilver**. The vendor’s system did not protect the signed record against post-execution alteration, and the post-execution audit trail maintained by the vendor showed that two Quicksilver employees had accessed the record after it was first saved and submitted for storage.
Original Record vs. Proof of Process

Person v. Google, Inc.
The court relied on proof of process as opposed to proof by the document itself to support defense.

Bar-Ayal v. Time Warner Cable Inc.
Clearly presented agreements will be enforced unless unconscionable. Court accepted a re-enactment of the agreement formation process (where the plaintiff had to click on the Accept button eight times) in order to refute the plaintiff’s claim that he never saw the agreement.

Hook v. Intelius
Evidence of process alone is sufficient to support a finding that the process used is standard in the industry and produces an accurate result.
Attribution

1. Signer Identity

- **Primary**
  - Email Address
  - DocuSign Account
  - Federated/SSO

- **Multifactor add-ons**
  - Access Code
  - SMS
  - Phone
  - Social ID
  - Digital Certs

- **KBA or In Person**
  - ID Check
  - Electronic Notary

- **Standard Method**
- **Enterprise Add-On**

Industry-Leading Choice of Authentication Options

2. Audit Trail
Record Integrity

Restricted Access

- Tags
- Email Access Code
- Recipient Roles

- Hashing and Encrypting
- Tamper Evident

Security Certifications

- Tags
- Email Access Code
- Recipient Roles

- Hashing and Encrypting
- Tamper Evident
Questions?