Electronic Signatures in Banking

Andrea J. Shaw, Esq
Business Law / Financial Services
April 11, 2019
Today’s Agenda

Included – Learning & Fun!
1. What is an “Electronic Signature”
2. Select State and Federal Laws
3. Esign Best Practices
4. Record Retention

Not Included:
1. Electronic notarization
2. Complete discussion of FFIEC Guidance
3. Complete discussion of Privacy laws
What is an Electronic Signature
Electronic Signature - Definition

An Electronic Signature is:
A sound, symbol or process,
Either attached to, or logically associated with, a Record AND
Created, adopted by the signer, with the intent to sign the Record.
Electronic Signature – Definition

Examples:
• Typed name;
• Click-Through
• Recorded Voice;
• Personal Identification Number;
• Password;
• Biometric measurement;
• Digitized image of a handwritten signature.
Signature vs Authentication

- Signature tells us that you agree to the transaction;
- Authentication tells us you are who you say.
Statutory Overview – State & Federal Laws
Uniform Electronic Transactions Act ("UETA")

- Uniform law proposed in 1999;
- Goal of the UETA was to remove barriers to electronic commerce and to provide parties a legal framework for using electronic signatures and records in business transactions;
- Under the UETA, electronic records and signatures have the same legal effect as paper contracts and handwritten signatures;
- All states except Illinois, New York and Washington have adopted some version (these states have laws on electronic signatures, but did not adopt a version of UETA);
- UETA generally does not apply to transactions governed by:
  - Laws relating to the creation and execution of wills, codicils, or testamentary trusts.

- Maine: [https://www.mainelegislature.org/legis/statutes/10/title10ch1051.pdf](https://www.mainelegislature.org/legis/statutes/10/title10ch1051.pdf)
Electronic Signatures in Global Commerce ("ESIGN")

- Enacted June 30, 2000;
- Effective October 1, 2000;
- ESIGN adopts the simple principle that electronic signatures and records should be accorded the same legal status as ink signature and paper records.
- ESIGN does not change the underlying substance of any law within its scope; instead, it affects only the medium for execution and delivery of writings;
- Commercial and consumer transactions have different requirements;
- ESIGN may preempt state law;
- Exempts similar transactions as UETA:
  - Laws governing wills, codicils, or testamentary trusts;
  - Laws governing adoption, divorce or other family law matters.
Electronic Signatures in Global Commerce (‘‘ESIGN’’)

Trigger for Consumer Provisions: Disclosure required to be provided ‘‘in writing’’;
1. Disclosure Requirements:
   1. Availability of Paper Delivery or Paper Copies (and consequences);
   2. Consent Choices;
   3. How Consumer can withdraw Consent (and consequences);
   4. Hardware/Software Requirements;
   5. Affirmative Consent;
   6. Required to keep Consumer updated if the above changes.

2. ‘‘Demonstrable Consent’’
   - Put ‘‘secret code’’ in document format that will be the subject of the transaction and have
     Consumer send code back (track and retain proof of receipt);
   - Use same coding ‘‘language’’ (ie – if transaction is in HTML, disclosure must be in HTML).

3. Consequences for Non-Compliance with ESIGN – it’s like the required disclosure was
   NEVER provided.
Other Statutes

- **Maine Digital Signatures Act;**
- **Controlling the Assault of Non-Solicited Pornography And Marketing Act (CAN-SPAM):** Requires senders to provide an opt-out of marketing emails and prohibits false or misleading email header information and deceptive subject lines;
- **Digital Millennium Copyright Act (DMCA):** Protects ISPs from copyright infringement liability by their users;
- **Federal Trade Commission Act (FTCA):** Prohibits unfair and deceptive acts and practices;
- **Children's Online Privacy Protection Act (COPPA):** Governs the online collection of personal information from children under 13 years of age;
- **Americans with Disabilities Act (ADA):** Prohibits the owner of a place of public accommodation from discriminating on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.
General Contract Clause

No Consumer Disclosure Required in Writing

1. **Electronic Signatures.** Each party agrees that the electronic signatures[, whether digital or encrypted,] of the parties included in this Agreement are intended to authenticate this writing and to have the same force and effect as manual signatures.

   Electronic signature means any electronic sound, symbol, or process attached to or logically associated with a record and executed and adopted by a party with the intent to sign such record[, including facsimile or email electronic signatures.}
Authentication

Are you really you?
Authentication

Traditional: Personal Appearance with Identification;

Electronic:
1. Self Authentication – “I swear I’m me”;
2. Logical Authentication – the area code and zip code are consistent;
3. Negative Authentication – looks to see if information provided is associated with known fraud;
4. Third-Party Authentication – Consumer Reporting Agencies sell products;
5. Positive Authentication – Information provided matches other known information about person.
Authentication

Considerations:
1. Single transaction or multiple;
2. Will transaction be likely to attract fraudsters;
3. Potential value/loss from each transactions;
4. Will there be limits or controls in place down stream to help control risks;
5. Is this transaction establishing a “new customer” so BSA CIP is required?
Electronic Signature
How to Electronically Sign

- Type your name (email)
- Click “I accept” (clickwrap)
- Proceed with the next action (website terms of use)
- Print the document, sign it and scan it
- Use software to create a digital signature
Digital Signatures

- **Digital Signature**

Anyone digitally signing a document needs a digital certificate; the certificate being unique to that individual. The certificate contains a public and a private key – known as a ‘key pair’. *Digital signature* software works by performing these steps:

1. The software creates a ‘hash’ of the document content. Hashes are representations of the whole content, including images.
2. The signatories certificate is then used to encrypt the hash. This combination of hashing and encryption creates an intrinsic connection between the document and the signatory; digital signing in this way, ties the two together.
3. The document hash is checked using the public key of the certificate to make sure it can be decrypted. It can only be decrypted if the user’s public key matches the private key used to encrypt the document.
4. When the signature is checked using the digital signing software, the original document is hashed again and both the original and signed hash are crosschecked. If there’s a difference between them, then the signature is invalidated. Because a *digital signature* is effectively, ‘wrapped up’ in the content of the document, it means that if anyone tries to change anything about that document content, the signature will also change. It effectively invalidates the signature and indicates that the document has been tampered with.
Electronic Signature vs Digital Signature

• Which should you use when?
• Depends on the transaction
Record Retention
- **Bank Record Retention:**
  - Electronic records generally permitted so long as the Bank can rely on the information;
  - Information must accurately reflect the contract or other record and it is accessible to all persons who are legally entitled to access that information;
  - Can be a form that allows for reproduction;
  - **Maine Law Practice Point:** it is debatable whether electronic mortgages/notes are sufficient so we recommend maintaining paper versions in addition to electronic copies.

- **Consumer Record Retention**
  - Generally acceptable if it is in a form that the Consumer can download and save or print.
Electronic Signature Implementation
Best Practices
Best Practices

- Research potential vendors and understand how they meet UETA and ESIGN requirements;
- Pick one low risk product to launch;
- If utilizing email, institute a “bounce back” management process;
- Implement an Electronic Signatures Policy

- Have a Data Breach action plan that reflects current use of electronic signatures/transactions;
Questions?

Andrea J. Shaw, Esq
Ashaw@BernsteinShur.com
207-228-7187

The materials provided in this presentation are for informational purposes only and not for the purpose of providing legal advice. The opinions expressed at or through this presentation are the opinions of the individual presenter/author and may not reflect the opinions of the firm.