

Top Ten E-Accidents Waiting to Happen to Financial Institutions

Are you up-to-date on compliance with the many e-commerce laws that affect financial institutions? Most institutions are not. *The Law of Electronic Commercial Transactions*, by Raymond T. Nimmer and Holly K. Towle, provides in-depth information for avoiding these costly pitfalls.

- 1. Failure to comply with UETA¹ and E-Sign.** Chapters 4 and 11 deal with special rules for e-dealings set in these new laws. Some financial institutions routinely fail to meet them! Examples:
 - A financial institution application form saying “E-Mail Address” is at risk if the institution uses that address to meet a law requiring it to send notice of default.²
 - If a law requires a customer to “sign” a disclosure or waiver, is an “I Agree” button really a “signature” or is it a mere consent not meeting a “signature” requirement? Chapter 4, Section 4.18 explains the potential difference.
- 2. Failure to comply with E-Sign³ 101(c) in consumer transactions.** Chapters 4 and 11 explain this special federal rule, which must be met before a financial institution may substitute an e-disclosure for a disclosure otherwise required to be “in writing” (on paper, such as in some lending and insurance transactions). Most institutions do not fully comply with the rule or get the timing wrong.
- 3. Failure to modernize contract language.** Financial institution contracts are full of “boilerplate” language drafted decades ago that no longer works in an “e” economy. Examples:
 - Amendment clause requiring “written” or “signed written” amendments — Chapters 4 and 13 explain that an e-mail from a bank employee can easily meet that requirement even if the bank thinks paper and a formal, inked signature is required.
 - A clause in a 15-page merchant processing contract saying that the 15 pages are the “entire agreement of the parties regarding its subject matter” is likely wrong: the bank probably allows the merchant to log into a bank site to review and manage daily settlements and processing issues. The terms of use and disclosures on that site are part of the subject matter too, and their existence may vitiate any effectiveness of the clause (unless appropriately revised).
- 4. Failure to keep up with contract law rules developing outside the banking universe.** Examples are concepts of “opportunity to review” and “shrinkwrap” or “layered contracting” (such as for software licenses involving terms delivered after partial contract formation). Chapter 5 provides a primer on modern contract rules, but many bank contracts continue to reflect outdated rules.⁴
- 5. Failure to comply with e-records rules.** Chapters 4 and 13 discuss new rules and legal defenses impacting e-records but not paper records. Failure to comply can invalidate the e-record, preclude admission into evidence, or create liability in litigation when records must be produced. Many financial institutions are aware of the new litigation rules

1. Uniform Electronic Transactions Act—this is a state statute in about 46 states that applies to state law rules in addition to E-Sign.

2. UETA requires e-mail address fields to specify the type of notices that will be sent to that address and in the example, the institution did not do that; UETA also defines “send” in ways that the institution may want to vary by contract.

3. Electronic Signatures in Global and National Commerce Act—this is a federal statute.

4. E.g., commercial merchant processing agreements in which operating rules or other details are not timely provided; consumer payment card applications where even if federal disclosure rules are met, contract or UDAP (unfair or deceptive acts or practices) rules often are not.

but are not paying attention to the new (or old, but newly nuanced) substantive and evidentiary rules. The book deals with all of them, including illustrative case law.⁵

6. **Failure to fully accommodate nuances of the information economy.** Chapters 2 (Intellectual Property Basics), 3 (Property Rights beyond IP), and 10 (Liabilities of Information Providers) deal with issues unique to an information economy as opposed to a “goods” economy. Example: is a plastic gift card sold to a consumer a “good” governed by UCC Article 2 contract rules (including Article 2 implied warranties and damages) and is it a “first sale” under copyright law of the software in the card? The answers matter, but most banks have not dealt with the issues.
7. **Failure to track developing duties.** Chapters 4 (Electronic Transaction Validation Rules) and 6 (Attribution) deal with rules for “knowing your customer” that go beyond the USA PATRIOT’s act (which is the focus of most financial institution compliance). Example:
 - Combining Exhibit 6.1 (FFIEC guidance essentially prohibiting single-factor authentication for material monetary transactions) with Section 6.05 (UCC Article 4A rule requiring banks to provide commercially reasonable security procedures) should encourage a financial institution to provide more than single-factor authentication⁶ for Article 4A transactions. But many do not, and the first lawsuit for money lost by a commercial customer has been filed.
8. **Failure to track developing liabilities.** Chapters 10 (Liability of Information Providers), 8 (Terms of Use), 2 (Intellectual Property), 3 (Property Rights beyond IP), and many other chapters track emerging risks and liabilities that did not exist or were not relevant a decade ago. Banks tend to focus on “banking” literature instead of on “general” developments, but general developments matter and *The Law of Electronic Commercial Transactions* tracks them. Example:
 - Bank commercial customer terms of use often count a notice posted on the site as notice to the customer. Chapter 8 includes discussion of a Ninth Circuit case concluding that at least in some contexts such a posting would be unconscionable; even if not, if the notice were posted to meet a contractual or legal “delivery” requirement, posting would not be “delivery” under UETA (see Chapters 4 and 11).
9. **Failure fully to consider state data security laws because of a too-narrow focus on federal laws.** Although Chapter 12 deals with the federal Gramm-Leach-Bliley Act applicable to financial institutions, that act does not preempt more protective state laws. Chapters 12 (Privacy), 15 (Identity Theft), and 16 (Security) deal with many state laws in the data protection area, but many financial institutions are not sufficiently aware of them.
10. **Failure to consider technological differences.** Some financial institutions assume that, once the leap is made into e-commerce, one e-size fits all. That is not the case:
 - Marketing and privacy rules distinguish between types of technologies used, such as marketing sent to an e-mail vs. mobile service address, collection of biometric information vs. other personal data, and use of RFID technologies or behavioral advertising technologies.
 - Application of contract law and UDAP rules vary among customers signing up with cell phones, Blackberries or full desktop computers — what is conscionable or printable for one type of hardware might not work for others.

The Law of Electronic Commercial Transactions outlines basic rules that can be adapted to technologies and hardware used; it also tracks special rules for particular technologies.

5. It cites, for example, *In re Vee Vinhnee*, 336 BR 437 (9th Cir. 2005) (American Express denied recovery against debtor because AmEx did not properly establish an evidentiary foundation for the accuracy of its electronic record-keeping system).

6. An example would be two-factor authentication, such as requiring the customer to enter a password (something the customer “knows,” factor 1) and to use a card or other token to log into the system (something the customer “has,” factor 2).