KELLEY DRYE

Billing and Financial Privacy Considerations for Product Sales

(Excerpts from KDW CLE, NY, May 2007)

KELLEY DRYE

This presentation is designed to provide an overview of billing and general financial considerations for merchant sales. References are intentionally general and may include summary statements based on a broad reading of applicable rules and statutes. This document should not be substituted for advice of counsel on specific sales models.

Overview

- The basics
- Choice of payment
- Applicable law
- Special considerations for preauthorized/recurring bill
- Processing relationships
- Storing/Sharing payment information
- Getting rid of old information
- Top 10 questions to always ask

KELLEY DRYE

The Basics

- Who is selling the product or service (merchant of record)?
- Who is obtaining billing authorization?
- What billing methods will be accepted (Invoice only, credit card only, credit/debit, credit/debit/checking?)
- What's the nature of the billing relationship (single credit/debit, recurring billing)
- Who is settling transactions?

KELLEY DRYE

Choice of Payment

- Credit
- Debit
  - Debit Card
  - Direct Debit (Checking)
- Other
  - Invoice
  - Phone Bill
  - Prepaid/Gift Cards

KELLEY DRYE

Applicable Law

Charge
(Credit Cards)

- Federal Law
  - Truth in Lending Act, Regulation Z
- Association Rules
  - Card Association Rules (Visa, MasterCard, Am. Ex., etc.)

Electronics Fund Transfer
(Debit Cards, Checking Accounts)

- Federal Law
  - Electronic Funds Transfer Act, Regulation E, ESIGN
- Association Rules
  - National Automated Clearing House Association "NACHA" Rules

Agency Orders

FTC Consent Decrees (?)

State Attorneys General Letter of Voluntary Compliance (?)

KELLEY DRYE

Credit Cards: Association Rules

- All Charges
  - Authorization process must be consistent, secure, and defensible against cardholders, issuing banks, payment processor and card associations.
  - Authorization must comply with Card Association Rules
  - Need to take into account one-time v. recurring charge requirements
  - Receipt requirement
  - Provide consumer choice (debit/credit)
  - Evidence of Authorizations must be maintained in accordance with applicable record retention requirements
  - All material terms of sale must be disclosed in advance of requesting billing information.

KELLEY DRYE

Debit Cards/Checking: EFTA/Reg. E, NACHA Rules

- One Time Transfers
  - Authorization process must be consistent and authorization must be defensible to account holders, associated financial institutions, payment processor and NACHA.
  - Information must be maintained in accordance with appropriate record retention policy.
  - All material terms of sale must be disclosed in advance of requesting billing information.

KELLEY DRYE

Debit Cards/Checking

- Pre-Authorized (Repeat) Transfers – Additional Requirements
  - Authorization must be signed or similarly authenticated (in both cases, consent must evidence authorization and authenticate identity of signer).
  - If “signed” electronically, then ESIGN applies
  - ESIGN requires the “signed” authorization to be in a printable, downloadable, savable form.
  - 10 day advance notice of any increase or decrease in amount billed under preauthorization.

KELLEY DRYE

ChargeBacks

- Must have a process (generally accommodated through payment processor) to reverse charges/debits made in error, including internal processes to locate and retrieve evidence of consumer authorization to bill.

KELLEY DRYE

Other

- Invoice
- Payment Service
- Phone Bill

KELLEY DRYE

Payment Processing: Supporting Your Model

- Retaining a payment processor
- Obtaining merchant ID(s)
- Contracting to accommodate payment services
- In-house or vendor customer support

KELLEY DRYE

Storing/Sharing Payment Information

- Data Security
  - Association protocols and general security considerations
- Data Sharing
  - Sharing with affiliates
  - Sharing with non-affiliates
  - Association prohibition on passing card numbers

KELLEY DRYE

Data Security: PCI and Related Protocols

The Payment Card Industry (PCI) data security protocol requires all merchants to comply with association-promulgated data security standards. Visa and MasterCard both require PCI compliance (either self audit or third party audit, depending on size of merchant and number of transactions processed). Separate protocols (e.g., CISP for Visa) may also apply.

KELLEY DRYE

General Security Considerations

- Limit employee access to individuals with “need to know”
- Password protection for online access
- Avoid unencrypted transmission
- Avoid housing payment information on shared files/servers/data bases
- In office policy for limited access to receipts, faxes or other hard data.
- Limit portability (no laptop/Blackberry access)

KELLEY DRYE

Sharing Billing Information: Governing Authorities

- Card Association Rules (Security and Data Sharing)
- Federal Statutes (Data Sharing)
- Gramm-Leach Bliley Act (GLB)
- Fair Credit Reporting Act (FCRA)
- State Statutes
- Your Own Privacy Policy(s)

KELLEY DRYE

Sharing with Non-affiliates: Gramm-Leach-Bliley

- GLB permits sharing of non-public personal financial information between non-affiliated third parties with consumer notice and opt out.
- GLB prohibits sharing account numbers (ex: credit card numbers) with non-affiliated third parties, even with consumer consent.*
- GLB does not address information sharing between affiliates.
- *Limited exceptions for: (i) disclosure to agencies to conduct marketing on institution's behalf, (ii) sharing with participants in a private label credit card program or other affinity program provided participants are identified to the consumer at program registration, and (iii) sharing encrypted numbers used for tracking purposes, without means to decrypt.

KELLEY DRYE

Sharing with Affiliates: Fair Credit Reporting Act

- As amended by the FACT Act, effective December 2003, the FCRA prohibits affiliated companies from sharing financial transaction or experience information for marketing purposes without written notice and an opt out option for effected consumer(s).
- NOTE: Prior to FACTA, merchants could share their own consumer transaction information without restriction.

KELLEY DRYE

Card Association Prohibition on Affiliate AND Non-Affiliate Sharing for Card Numbers

» Card Association (AMEX, Visa, MasterCard, etc.) Merchant rules generally prohibit a merchant from using credit/debit card information for any purpose other than settling consumer purchases. Merchants are generally subjected to Association Rules by reference in their agreements with their payment processor.

KELLEY DRYE

State Laws

» A handful of states have statutes targeting identity theft that dictate when/how financial account information may be shared. State statutes for, at a minimum, the states in which potential sharing partners are incorporated should be reviewed to assure there are no specific prohibitions.

KELLEY DRYE

Internal Privacy Policy(s)

- All merchants must abide by their own privacy policies as they pertain to sharing transaction histories or customer financial information.
- Example: If your privacy policy states you will not share customer information with any third parties. This broad prohibition would include all types of information and would encompass sharing with an affiliated company.

KELLEY DRYE

What to Do with Old Billing Information

- Retain evidence of billing authorizations in a secure area and accordance with Association requirements and consistent with internal data retention policies.
- Delete ALL specific payment information as soon as practicable and no longer than required to verify authorization or necessary to address residual issues upon termination of consumer relationship

KELLEY DRYE

Top 10 Questions to Ask

- Who is selling the product service (merchant of record)?
- Who is obtaining billing authorization?
- What billing methods accepted (Invoice only, credit card only, credit/debit, credit/debit/checking?) and with proper authorization?
- What's the nature of the billing relationship (single credit/debit, recurring billing)
- Who is settling transactions?
- Are all relationships (billing agent, processor, vendor) properly documented to reflect roles of parties and parties' data security obligations?
- Where is data being collected/stored – data security controls?
- Who has access to data?
- Do you anticipate affiliate or non-affiliate data-sharing, and if so, does sale incorporate required opt-in/opt-out notices?
- Where does the payment information go after sale or the end of the relationship?

KELLEY DRYE

Joel Hewer

Kelley Drye and Warren LLP

Washington, DC

202/342-8520

jhewer@kelleydrye.com

KELLEY DRYE