Accepting Credit Card Payments

By Erin F. Fonte and Jacqueline M. Allen

More and more attorneys and law businesses are accepting credit card payments from their clients to pay for legal fees. While credit card payments offer many benefits, they also carry risks that are not present with other forms of payment.

How many times have you heard a client tell you "the check is in the mail" only to never receive a payment? With credit cards, you can process a payment from a client on the spot. You no longer have to wait for the check to come in through the mail or take the check to the bank to deposit it. Credit card payments also provide immediate confirmation that the payment is good, whereas checks may take days to post and can be returned weeks or even months later. Companies such as Square even allow you to process credit card payments using your mobile phone now (*e.g.*, for payment on a contingent case at the courthouse immediately after the judge hands down the verdict on your case).

But there are risks unique to credit cards that are not present with other forms of payment. For each credit card transaction you initiate, the processor usually accesses a percentage of that payment as a fee for using the processing service. Clients can also "chargeback," or dispute, credit card payments after the payment has been made. PCI DSS standards, discussed further below, may also seem intimidating and discourage many from accepting credit card payments.

Should you choose to accept credit card payments from your clients, this article offers guidelines for doing so.

How to Process Credit Card Payments

The American Bar Association and many state bar associations have affirmed that lawyers may accept credit card payments for legal fees.[1] Recall, however, that payments (including credit card payments) made for advance legal fees must be processed differently than payments for fees already earned though. Payments for advance legal fees must be credited to a client's trust account until the fees are earned, while payments for fees already earned must be credited to an attorney's operating account. Certain types of advance fee (*e.g.*, flat fees) may, of course, be considered an attorney's property upon receipt and be placed in the operating account. Check

[1] *See* ABA Formal Opinion 00-419 (2000), which withdraw a number of earlier ABA opinions on legal fee financing issues, but stated that the use of credit cards is permissible so long as the attorney's promotion of the fact that he or she accepts credit cards is not false, fraudulent, or misleading.

your state's rules and ethics opinions to determine how certain advance fees are characterized in your state.

When choosing a vendor to process your credit card payments, be sure the company is capable of separating earned and unearned fees. Square and PayPal, while both attractive options for accepting credit card payments in most industries, may not comply with your state bar's trust account rules in all situations because they may not allow you to separate operating account income from trust account income.

Another important thing to consider during the initial set up phase with a credit card vendor is the name in which you will be set up. It is important to use the exact legal name found on your IRS records and not an abbreviation or acronym. A 2012 change to the tax code now requires credit card companies to verify and match your federal tax identification number and legal name on your merchant account to IRS records. If the number and name to do not match exactly, the IRS may impose a 28% withholding penalty on all credit card transactions.

Credit Cost Processing Fees

The cost of credit card processing varies by vendor, but vendors are typically paid on a per transaction basis. These amounts can range anywhere from 0.5% to 5% of the payment amount. When selecting your credit card vendor, beware of contracts with promotional prices that apply only for a period of time but significantly increase after an initial honeymoon period and lock you into the contract for an extended period of time.

Federal law and some state laws also restrict merchants from imposing minimum fees for credit card transactions. For instance, the federal Dodd Frank Wall Street Reform and Consumer Protection Act permits a merchant to set a minimum dollar amount for a credit card payment, so long as the amount does not exceed $10. Certain states, such as Texas, also prohibit merchants from charging customers a surcharge to pay by credit card.

Keeping Credit Card Information on File

You may need the ability to recharge a client's credit card if you plan to bill that client on a monthly recurrent basis, which may necessitate the need to keep a card number on file. Keeping credit card information on file, however, may pose data security risks depending on how the card information is stored. Maintaining paper copies of client credit card numbers, such as from the traditional credit card machines, poses the greatest risk. Using a secure, web-based solution that encrypts all credit card information provides a less risky alternative.

Depending upon the way in which credit card information is stored, state data security notification obligations may be triggered if the client's credit card information is compromised. For instance, in Texas, if a consumer's credit card number is compromised in combination with certain other information (*i.e.*, the consumer's first name or first initial, last name, and any required security code, access code, or password that would permit access to the financial account), you would have an obligation under Texas state law to notify the affected consumer(s) and take certain remedial actions. For credit card information that is in an encrypted form, however, a compromise of this information would not trigger data breach notification obligations in most states.

PCI/DSS Standards

PCI-DSS, or the Payment Card Industry Data Security Standards,[2] is the payment card industry's set of requirements for processing, storing, and transmitting credit, debit, and prepaid card information in order to maintain a secure environment. PCI applies to all merchants, regardless of the size or number of transactions the merchant processes. If you accept credit card payments, you are subject to PCI, even if you use a third-party payment processor.

PCI is enforced by the payment brands (*i.e.*, American Express, Discover, JCB, MasterCard, and Visa International). These brands may impose fines for PCI compliance violations only on acquiring banks. The banks, however, will likely pass these fines on to the merchant and the fines may reach upwards of $5,000 to $100,000 per month.

PCI DSS prohibits the full primary account number (PAN) (usually a 16-digit number on the card) from being displayed for any credit, debit, or prepaid card number that is stored. Instead, only the first six and last four digits of the account number may be displayed; the remaining digits must be masked. State laws may also impose limitations on printing the account number on a receipt. For instance, Texas law prohibits a merchant from printing any more than the last four digits of the PAN on the customer's receipt.[3] The merchant is also prohibited from printing the card's expiration date on the receipt in Texas.

PCI DSS imposes additional requirements based on each merchant's Visa transmission volume in a 12-month period, including credit, debit and prepaid card payments. The lowest tier, Level 4, includes merchants processing fewer than 20,000 Visa e-commerce transactions per year and

---

[2] The PCI Data Security Standards can be found here: https://www.pcisecuritystandards.org/security_standards/index.php.

[3] Tex. Bus. & Comm. Code § 35.58.

all other merchants processing up to 1 million Visa transactions per year, regardless of acceptance channel. A Level 4 merchant, for example, must:

1. Determine which PCI Self-Assessment Questionnaire (SAQ) it must use to validate compliance. PCI DSS provides a chart to help you determine which SAQ you must use: https://www.pcicomplianceguide.org/wp-content/uploads/2014/03/PCI-3.0-SAQ-Chart.jpg.
2. Complete the SAQ according to its instructions.
3. Complete and obtain evidence of a passing vulnerability scan with a PCI SSS-Approved Scanning Vendor (ASV), if applicable.
4. Complete the relevant Attestation of Compliance.
5. Submit the SAQ, evidence of a passing scan (if applicable), and Attestation of Compliance to your acquirer.

Due the complexity of the PCI DSS Standards, be sure to verify any credit card vendor you use is PCI-DSS compliant and the contract between you and the vendor states that the vendor will maintain PCI compliance.

About the Authors

Erin Fonté is a Member at Dykema Cox Smith. Erin practices in the firm's Financial Industry Group and Privacy, Data Security, and E-Commerce Group. She is also a Certified Information Privacy Professional as certified by the International Association of Privacy Professionals (IAPP).

Jacqueline Allen is an Associate at Dykema Cox Smith, is a member of the firm's Financial Industry Group and Privacy, Data Security, and E-Commerce Group, and is also an IAPP Certified Information Privacy Professional.