What follows is the questionnaire which will apply for all courts which do not use Judici to accept payments "on premises" (see http://www.goodinassociates.com/client-wiki/Wiki.jsp?page=Merchant%20compliance%20with%20PCI%20standards for more on that).

Goodin's guidance on completing this questionnaire is shown in italics.

This material is provided on an "as-is basis". GAL does not warrant that this it is accurate or complete.

How to Complete the Questionnaire

.
.
.

Questionnaire Reporting

.

.

.

APPROXIMATE NUMBER OF TRANSACTIONS/ACCOUNTS HANDLED PER YEAR: Please enter a number (i.e. enter "5000", not "five thousand")	Ask Goodin if you don't know

BRIEF DESCRIPTION OF YOUR BUSINESS:
Please explain your business' role in the payment flow. How and in what capacity does your business store, process, and/or transmit cardholder data?

We do not store, process or transmit cardholder data on premises. That function is outsourced to a third-party provider. Aside from cc'd e-mail copies of confirmations and receipts which do not contain cardholder data, we are not involved with the payment process- we simply receive the associated bank deposits.

LIST ALL THIRD PARTY SERVICE PROVIDERS (Select "None" if not applicable.)

Payment Gateway	*Goodin/Judici*
Web Host	*None (no separate host for your website- Goodin does it)*
Shopping Cart	*None- Judici does not use any shopping cart*
Co-Location	*None- "co-locate" means to put a web server which YOU own in some other location to run your website from. But the court doesn't own the Judici web server.*
Point-of-Sale Terminal	*None- Judici is not integrated with any terminals*
Payment Application	*Mainstreet Softworks- Monetra (the non-CardShield version)*

Eligibility to Complete SAQ A

Merchant certifies eligibility to complete this shortened version of the Self-Assessment Questionnaire because:

☐ Yes	Merchant does not store, process, or transmit any cardholder data on merchant premises but relies entirely on third party service provider(s) to handle these functions; *If you do not use Judici to accept (and "transmit") payments "on premises", this is true. See http://www.goodinassociates.com/client-wiki/Wiki.jsp?page=Merchant%20compliance%20with%20PCI%20standards for more on this*
☐ Yes	The third party service provider(s) handling storage, processing, and/or transmission of cardholder data is confirmed to be PCI DSS compliant; *Goodin is required by the card companies to certify its PCI compliance every year*
☐ Yes	Merchant does not store any cardholder data in electronic format; and *Judici doesn't store cardholder data at the court. In the very rare cases when a customer contacts the court, rather than Judici, for customer service, they might **try** to give you their cardholder information by email or phone. You should simply refuse that info and direct them to support@judici.com*
☐ Yes	If Merchant does store cardholder data, such data is only in paper reports or copies of receipts and is not received electronically. *Although Judici does NOT store cardholder data at the court, there is no choice but to answer "Yes" if you want to be certified compliant.*

Merchant Attestation

☐ Yes	All information given to SecurityMetrics for PCI scoping, information provided in this SAQ and in this attestation fairly represents the results of my assessment.
☐ Yes	I have read the PCI DSS and I recognize that I must maintain full PCI DSS compliance at all times.
☐ Yes	PCI DSS Self Assessment Questionnaire A, Version 2.0 was completed according to the instructions therein.

Restrict physical access to cardholder data	Click answer boxes below	
Judici does NOT store cardholder data at the court on ANY media (hard drive, paper, e-mails, etc.), so there shouldn't be anything at the court which needs to have its access restricted! But there is no choice but to answer "Yes" to the Section 9 questions if you want to be certified compliant.		
9.6 Are all media physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes)?	**YES**	NO
9.7.a Is strict control maintained over the internal or external distribution of any kind of media?	**YES**	NO
9.7.b Do controls include the following:		
9.7.1 Is media classified so the sensitivity of the data can be determined?	YES	NO
9.7.2 Is media sent by secured courier or other delivery method that can be accurately tracked?	YES	NO
9.8 Are logs maintained to track all media that is moved from a secured area, and is management approval obtained prior to moving the media .especially when media is distributed to individuals)?	YES	NO
9.9 Is strict control maintained over the storage and accessibility of media?	YES	NO
9.10 Is all media destroyed when it is no longer needed for business or legal reasons?	YES	NO
9.10.1 Is destruction performed as follows:		
9.10.1.a Are hardcopy materials cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?	YES	NO

9.10.1.b Are containers that store information to be destroyed secured to prevent access to the contents? (For example, a "to-be-shredded" container has a lock preventing access to its contents.)	YES	NO

Maintain a policy that addresses information security for all personnel

12.8 If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows:

12.8.1 Is a list of service providers maintained?
For Judici e-pay, Goodin is the only service provider you have a contract with. That's your list.

12.8.2 Is a written agreement maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess?
Goodin is responsible for the security of the cardholder data we possess

12.8.3 Is there an established process for engaging service providers, including proper due diligence prior to engagement?
*If you hire a service provider other than Goodin to collect credit card payments for you, you should have a procedure to make sure that **they** are PCI compliant.*

12.8.4 Is a program maintained to monitor service providers' PCI DSS compliance status at least annually?
Goodin is required to recertify our compliance to the card companies on an annual basis.