LawPay®

Legal Billing Templates

Building trust with clients is crucial for your firm and its reputation. One of the easiest ways to enhance the client experience is to clearly communicate your firm's guidelines during the intake process. For example, sharing your firm's approach to data security, commitment to IOLTA compliance, flexible payment offerings, and other essential policies shows your firm's dedication to providing an excellent experience from the start, increasing the likelihood that they'll use your services again if needed.

To help your firm ensure high client satisfaction, we've created a Legal Billing Templates packet to get you started. This packet includes:

- **A Sample Credit Card Authorization Form** *(pages 2-3)*
- **A Sample ACH/eCheck Authorization Form** *(pages 4-5)*
- **A Sample Employee PCI/Security Template** *(pages 6-16)*
- **A Sample Attorney Fee Agreement** *(pages 17-19)*

This way, you can simplify your intake process for both your firm and your clients, increasing productivity and profitability.

Want to see more ways to enhance your client experience through LawPay?
Schedule a demo today!

DISCLAIMER: The sample forms made available here are provided for individual review and analysis, and are delivered without warranty or representation of fitness for specific use or compliance. The receiver hereof is advised to make any necessary modifications or adaptations which may be required for the user's specific needs, or for compliance with the user's applicable practice rules or state statutes.

____

____

____

Client
Credit Card Authorization Form

In an effort to better serve our clients and simplify your billing experience, our firm offers online payments for your convenience.

CHARGE POLICY

ONE/FIRST TIME PAYMENT:

_______ (Initial) I hereby authorize______________________________to charge the balance currently due in the amount of $____________________.

FUTURE PAYMENTS (INSTALLMENTS):

_______ (Initial) I hereby authorize______________________________to charge the balance due each month, as reflected on the cardholder's invoice. Payment will be processed on the__________of each month for the prior month's fees.

FUTURE PAYMENTS (INSTALLMENTS):

_______ (Initial) I hereby authorize______________________________to charge my card in the amount of $__________on the__________of each month until the total sum of $__________has been paid.

POLICIES:

_______ (Initial) Payment is considered late after the________of the month. Any outstanding balance will be charged to the card on file. In addition, a late fee will be assessed in the amount of $__________.

_______ (Initial) Payment made for services delivered by this firm are non-refundable; you agree that you will first contact the firm, before disputing any charges with the card issuer.

_______ (Initial) In the case of retained services, any unused funds will be refunded to the card on file within __________days of__________________________.

_______ (Initial) Being the authorized cardholder or the Corporate Officer, by signing above I understand and agree to the terms set forth in this agreement, agree to pay, and specifically authorize the firm to charge my credit card for the services provided. I further agree that in the event my credit card becomes invalid, I will provide a new valid credit card upon request, to be charged for the payment of any outstanding balances owed.

CARDHOLDER INFORMATION

Cardholder Name: ____

Cardholder Billing Address: ____
____

Type of Card: □ Credit □ Debit □ VISA □ DISCOVER □ □ AMERICAN EXPRESS

Card Number: ____

** Per PCI Compliance guidelines, the last 4 digits may be recorded for verification purposes*

Expiration Date: ____________________ Security Code: ____________________

The undersigned guarantees performance of the financial provisions of this agreement.

Cardholder Name: ____

Cardholder Signature: __________________________ Date: ____________________

LawPay is a registered ISO of Synovous Bank, Columbus, GA., Fifth Third Bank, N.A., Cincinnati, OH, and Wells Fargo Bank, N.A., Canadian Branch, Toronto, ON, Canada.

Third Party Credit Card Authorization Form

____

____

____

In an effort to better serve our clients and simplify your billing experience, our firm offers online payments for your convenience.

3RD PARTY PAYMENT

______ (Initial) I, ______________________________, authorize ______________________________ to charge my credit card for the amount due of $______________________________.

______ (Initial) By signing I, ______________________________, understand I am paying for legal fees on behalf of, ______________________________, a client with this firm. I understand I will receive no direct benefit from this transaction or the legal services provided.

CARDHOLDER INFORMATION

Cardholder Name: ______________________________

Cardholder Billing Address: ______________________________

____

Type of Card: □ Credit □ Debit □ VISA □ DISCOVER □ □ AMERICAN EXPRESS

Card Number: ______________________________

** Per PCI Compliance guidelines, the last 4 digits may be recorded for verification purposes*

Expiration Date: ______________________________ Security Code: ______________________________

The undersigned guarantees performance of the financial provisions of this agreement.

Cardholder Name: ______________________________

Cardholder Signature: ______________________________ Date: ______________________________

____

____

____

Client
eCheck/ACH Authorization Form

In an effort to better serve our clients and simplify your billing experience, our firm accepts eCheck/ ACH payments for your convenience.

CHARGE POLICY

______ (Initial)

ONE/FIRST TIME PAYMENT:
I hereby authorize______________________________to charge the balance currently due in the amount of $______________________.

______ (Initial)

FUTURE PAYMENTS:
I hereby authorize______________________________to charge the balance due each month. Payment will be processed on the_________ of each month for the prior month's fees.

______ (Initial)

POLICIES:
Payment is considered late after the_________ of the month. Any balance will be charged to the bank account on file. In addition, a late fee will be assessed in the amount of $___________.

______ (Initial)

Payment made for services delivered by this firm are non-refundable; you agree that you will first contact the firm, before disputing any charges with the card issuer.

______ (Initial)

In the case of retained services, any unused funds will be refunded to the card on file within _________days of________________________.

______ (Initial)

A fee of $______________ will be charged for all returned checks.

______ (Initial)

Being the authorized account owner or the Corporate Officer, by signing above I understand and agree to the terms set forth in this agreement, agree to pay, and specifically authorize the firm to charge my bank account for the services provided. I further agree that in the event my banking information becomes invalid, I will provide updated payment information upon request, to be charged for the payment of any outstanding balances owed.

eCHECK

First Name: ______________________________ Last Name: ______________________________

OR

Account Holder Name (if Business): ______________________________

Account Type: □ Checking □ Savings

Account #: ______________________________ Routing #: ______________________________

Account Holder Signature: ______________________________ Date: ______________

LawPay is a registered ISO of Synovous Bank, Columbus, GA., Fifth Third Bank, N.A., Cincinnati, OH, and Wells Fargo Bank, N.A., Canadian Branch, Toronto, ON, Canada.

____

____

____

Third Party
eCheck/ACH Authorization Form

In an effort to simplify your billing experience, our firm accepts eCheck/ACH payments for your convenience.

3RD PARTY PAYMENT

______ (Initial) I, ______________________________, authorize ______________________________ to charge my bank account for the amount due of $______________________________.

______ (Initial) By signing I, ______________________________, understand I am paying for legal fees on behalf of, ______________________________, a client with this firm. I understand I will receive no direct benefit from this transaction or the legal services provided.

eCHECK

First Name: ______________________________ Last Name: ______________________________

OR

Account Holder Name (if Business): ______________________________

Account Type: □ Checking □ Savings

Account #: ______________________________ Routing #: ______________________________

Account Holder Signature: ______________________________ Date: ______________

LawPay is a registered ISO of Synovous Bank, Columbus, GA., Fifth Third Bank, N.A., Cincinnati, OH, and Wells Fargo Bank, N.A., Canadian Branch, Toronto, ON, Canada.

Table of Contents for Sample Employee PCI/Security Template

**The following Information Security Policy is intended to serve as an example of policies and procedures for a Level 4 merchant. These policies may not cover every requirement outlined by the PCI-DSS as applicable to your firm. It is the responsibility of the entity utilizing this tool to ensure full compliance with PCI-DSS regulations and proper use and implementation of its information security policy. AffiniPay, LLC and its partners will not be liable for your use of this Information Security Policy template, or for any misuse of this template or non-compliance with its terms by you or your employees.*

INFORMATION SECURITY POLICY

Introduction

PCI DSS 4.0 emphasizes continuous compliance, regular risk assessments, and real-time monitoring. Organizations must ensure ongoing evaluations and adaptations of this policy to align with PCI DSS 4.0 standards.

This policy covers the security of company or firm information, and each employee or contractor must read and sign a form verifying they have read and understand this policy.

Ethics and Acceptable Use Policies

[Enter Firm Name] (the “Firm”) expects that all employees conduct themselves in a professional and ethical manner. An employee should not conduct business that is unethical or illegal in any way, nor should an employee influence other employees to act unethically or illegally. Employees must refrain from using e-mail, internet or other Firm resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal. Furthermore, employees should report any dishonest activities or damaging conduct to an appropriate supervisor.

The Firm reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic.

Usage Policy

The Firm commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. Sensitive information must have adequate safeguards in place to protect our business, consumers, and to ensure compliance with various regulations.

Sensitive information is defined as any personal information (i.e.- name, address, phone number, e-mail, Social Security number, driver's license number, bank account, credit card numbers, etc.) or Firm information which is not publicly available (i.e.- clients financial information, employee information, schedules, technology, etc.). It is important that employees do not reveal sensitive information about our Firm or our customers to outside resources that do not have an established business need to know such information.

Employee Responsibilities:

- Handle Firm, customer, and / or cardholder information in a manner that fits with their sensitivity;
    - Do not disclose sensitive information unless there is a business need, and such disclosure is authorized.
    - Take reasonable precautions to ensure that sensitive information is not disclosed accidentally.
    - Attend training to understand the appropriate level(s) of sensitivity with which to treat various information
        - Example: A customer support phone number, vs. a Social Security Number.
- Keep passwords and accounts secure; this includes the expectation that Firm passwords are not stored on other computers or personal devices that are used to conduct Firm business when out of the office or working remotely.
- Always leave desks clear of sensitive data and lock computer screens when unattended;
- Use approved multi-factor authentication (MFA) solutions whenever accessing the cardholder data environment (CDE), whether remotely or within the internal network. This ensures an additional layer of security for sensitive data.

Prohibited Activities:

- Transmission of Sensitive Data via Insecure Channels:
    - Employees are strictly prohibited from transmitting cardholder data or other sensitive information through insecure channels such as email, chat, or messaging apps. This includes resolving customer service issues, billing disputes, or chargebacks. Instead, employees must use the firm's approved secure systems for any communications involving sensitive information.
- Storage of Sensitive Client Information:
    - The storage of sensitive client information (e.g., cardholder data) on employees' home computers, personal devices, or any system not approved by the firm is strictly prohibited.
- Unapproved Installation of Software/Hardware:
    - Employees are not permitted to install any software or hardware on Firm systems without explicit approval. All installations must be authorized by the appropriate personnel to ensure compliance with security policies.
- Use of Unapproved Devices or Media:
    - Employees may not use the following devices or media to access sensitive data without prior approval from the firm: Remote-access technologies, wireless technologies, removable electronic media, laptops, personal digital assistants (PDAs), smartphones, or tablets.
- Storing Sensitive Data Outside of Approved Solutions:
    - Storing sensitive cardholder data in any form outside of the firm's approved, PCI-compliant systems (including local storage on computers, external drives, or cloud storage) is strictly prohibited.
- Unencrypted Transmission of Sensitive Data:
    - Employees are prohibited from transmitting any sensitive data (e.g., cardholder data, personal information) over unencrypted or unsecured networks. Encryption must always be used for sensitive data transmission in line with PCI DSS guidelines.
- Sharing Credentials or Access Privileges:
    - Employees must not share their access credentials (e.g., passwords, two-factor authentication codes) with others. Each employee is responsible for protecting their login information and ensuring that it is not accessible to unauthorized individuals.

- Handling Cardholder Data Outside of Approved Processes:
    - Employees must never process, store, or handle cardholder data outside of the firm’s approved processes and systems. All cardholder data must be handled through the PCI-compliant systems provided by the firm, which automatically ensure secure storage and transmission.

Employees should report any Information security incidents without delay, to [INSERT Firm Incident response Contact information].

If you are unclear about any of the policies detailed herein you should seek advice and guidance from leadership.

Data Storage and Access

The Firm uses role-based access control; privileges are assigned to individuals based on job classification and function. To minimize risk, access to cardholder data is restricted to employees whose job functions require such access. Additionally, all users with privileged access to cardholder data must utilize multi-factor authentication (MFA) as required by PCI DSS 4.0. The firm will ensure that only individuals with a business need-to-know are granted access to sensitive information. Access controls will be implemented to ensure that cardholder data is only available to authorized personnel. No other employees, personnel, or third parties should have access to this confidential data unless they have a genuine business need. The Firm will implement basic monitoring tools or processes to track and review activity related to cardholder data. Alerts will be set up for critical events such as unauthorized access attempts, and logs will be retained and reviewed periodically in accordance with PCI DSS requirements.

- It is prohibited to store the contents of the credit card magnetic strip (track data) on any media whatsoever.
- It is prohibited to store the card validation code (3 or 4 digit value printed on the signature panel of the card) or PIN number on any media whatsoever.
- All sensitive cardholder data stored and handled by the Firm and its employees must be securely protected against unauthorized use at all times.
- The Firm must adhere to a strict data retention policy in line with PCI DSS 4.0 guidelines. Cardholder data should only be retained as long as it is necessary for legal, regulatory, or business reasons, and it must be securely destroyed or rendered irretrievable once it is no longer required.

- Any sensitive card data that is no longer required by the Firm for business reasons must be discarded in a secure and irrecoverable manner (E.g. Incineration, cross-cut shredding, etc.)
- The Firm will implement logging and monitoring mechanisms to track access to cardholder data. All access to systems that handle cardholder data will be logged to ensure that unauthorized access attempts or suspicious activity can be detected. Logs will be reviewed periodically and retained in accordance with PCI DSS requirements to support investigations of potential security incidents.

Visitor Access

Visitors must always be escorted by a trusted employee when in areas that hold sensitive cardholder information. A "visitor" is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the premises for a short duration, usually not more than a few days.

Sharing Sensitive Data: Duties and Responsibilities

Third Parties:

- A list will be maintained detailing all third parties, including service providers, that collect, store, process, or transmit card information, or with whom card information is shared. A full list of these third parties is detailed in Appendix A. *[NOTE: If LawPay is your only payments-related provider and you do not store PCI data in any other third-party services, you only need to list LawPay.]*
- The Firm will ensure a written agreement is in place with all Service providers that receive sensitive data. All such agreements will include:
    1. An acknowledgement that the Service Provider will be responsible for the cardholder data that the Service Provider possesses
    2. An agreement that Service Provider will comply with applicable card association security standards (PCI-DSS). Contracts with service providers must include clauses requiring regular audits and reporting to ensure adherence to PCI security standards, where applicable.
- Appropriate due diligence will be conducted prior to engaging any Service provider.
- The Firm will ensure that third-party providers are continuously monitored and reviewed for ongoing compliance.

Secure Transmission Practices:

- When a card number is displayed electronically or on paper, the card account number will be truncated by default.
- Media containing sensitive cardholder information is to be handled and distributed in a secure manner by trusted individuals.
  - Media is defined as any printed or handwritten paper, received faxes, floppy disks, back-up tapes, computer hard drive(s), etc.
- Cardholder data must be encrypted using end-to-end encryption (E2EE) when transmitted over untrusted networks, and tokenization should be implemented to protect sensitive data at rest. PCI DSS 4.0 requires that any transmission of sensitive data is secured by strong encryption methods.
- Media containing sensitive data must be logged, inventoried, and authorized by management before leaving the premises.
- If approved media containing sensitive data needs to be shipped, it will be done using a shipping method that can be accurately tracked, via a secure courier.

Disciplinary Action

An employee's failure to comply with the standards and policies set forth in this document may result in disciplinary action up to and including termination of employment.

Physical Payment Devices and Access

If the Firm elects to use any physical payment devices (Point-of-Interaction or POI devices), the Firm will maintain a basic record such devices, train its personnel on the use and security of such devices, perform periodic visual inspections of each POI device, and immediately report any suspicious findings to the appropriate service provider for further investigation. [NOTE: if you purchase a POI device from AffiniPay, we can assist you with understanding the PCI requirements applicable to such devices.]

Firewalls

The Firm will maintain a list of services, protocols, and ports for its firewall and router configurations. The firewall rules will be reviewed annually, or when there is a significant network change. If using a managed firewall service, the service provider will be responsible for ensuring firewall configurations comply with PCI DSS.

Wireless Networks & Connections

The Firm will segment wireless networks from the cardholder data environment using encryption (WPA3 or WPA2) and proper firewall rules. Wireless networks will be treated as external networks and will not have direct access to systems processing cardholder data.

Network Configuration

Vendor-supplied default accounts and passwords on critical systems (such as POS systems, firewalls, and routers) will be changed during installation. Default accounts will be removed or disabled if unnecessary to reduce potential security risks.

A simplified data flow diagram will be maintained to show the basic path of cardholder data through the Firm's payment systems. This diagram will be updated if significant changes to the systems or network occur.

Anti-Malware must be installed on all personnel computers and servers

All of the following apply: The anti-malware in use must

- Be kept current,
- Perform periodic scans,
- Generate audit logs,
- Be actively running,
- Not be able to be disabled or altered by users.

Users are made aware of appropriate response and reporting procedures if Anti-malware detects suspicious activity.

Security Awareness and Procedures

Keeping sensitive information secure requires periodic training of employees and contractors to keep security awareness levels high. The following Firm policies and procedures address this need;

- Hold [enter time interval (e.g. annual)] security awareness training for employees and contractors to review correct handling procedures for sensitive information.

- PCI DSS 4.0 requires that security awareness training be ongoing and adaptable to the evolving threat landscape. Employees and contractors must participate in role-specific training, as applicable, that is tailored to their interaction with cardholder data, and these sessions should be refreshed regularly to reflect new threats and compliance requirements.
- Employees are required to read this security policy and verify that they understand them by signing an acknowledgement form (see Appendix B).
- Background checks (such as credit and criminal record checks, within the limits of local law) will be conducted for all employees that handle sensitive information.
- Firm security policies must be reviewed annually and updated as needed.

Security Management/Incident Response Plan

The Firm's owner, manager, or designated employee will serve as the Security Officer responsible for communicating security policies and tracking adherence to policies. In the event of a security breach, this individual will oversee the execution of the incident response plan.

Incident Response Plan

1. If a compromise is suspected, alert the information Security Officer, [Enter Name].
2. The Security Officer, appointed personnel, and / or appointed third-party security partner(s) will conduct an initial investigation of the suspected compromise.
3. If a compromise of information is confirmed, the Security Officer will begin informing parties that may be affected by the compromise. If the compromise involves credit card account numbers, the Firm must perform the following:
   - Contain and limit the extent of the exposure by shutting down any systems or processes involved in the compromise.
   - Alert necessary parties (Merchant Bank, Visa Fraud Control, law enforcement).
   - Engage with security professional(s) to identify, contain and remediate affected systems and vulnerabilities
   - For additional details regarding Firm's incident response plan; please review Visa's Guide ***"What to do if Compromised"***
4. The Incident Response Plan (IRP) must be tested on a regular basis, and the results of these tests should be documented to ensure the Firm can quickly respond to breaches or compromises involving cardholder data. Testing should occur at least annually and after any significant changes to the cardholder data environment, per PCI DSS 4.0 requirements.

Appendix A:

Third party Providers That Collect, Store, Process, Transmit, Receive, or Have Access to Cardholder Data

Name of Third Party:	Date of agreement with provider	Type of Interaction(s) with Card Data	Date of Last PCI-DSS validation

Appendix B:

Employee Information Security Acknowledgement

Agreement to Comply with Information Security Policies

Employee Name: ____

Department: ____

Date: ________________________

I agree to take all reasonable precautions to ensure that Firm internal information, or information that has been entrusted to the Firm by third parties such as customers, will not be disclosed to unauthorized persons. At the end of my employment or contract with the Firm, I agree to return all internal or confidential information to which I have had access as a result of my position. I understand that I am not authorized to use sensitive information for my own purposes, nor am I permitted to provide this information to third parties without the express written consent of a firm owner or the designated Firm Security Officer.

I have access to a copy of the Information Security Policy, I have read and understand it, and I understand how it impacts my job. As a condition of continued employment, I agree to abide by the Information Security Policy and other information security requirements communicated to me from time to time. I understand that non-compliance will be cause for disciplinary action which may include dismissal and, if applicable, criminal and/or civil penalties.

I also agree to promptly report all violations or suspected violations of the Information Security Policy to the designated Security Officer.

X____

Employee's Signature

(This is a fee agreement template for hourly billing and not legal advice, please modify as appropriate and revise to include any local requirements.)

ATTORNEY FEE AGREEMENT

WHEREAS, [Name of Client] ("Client") desires to employ [Name of Firm or Attorney] ("Attorney") to represent him/her/they in the following legal matter:

[describe matter] and to represent Client in any and all claims and defenses to which the client may be entitled in connection therewith;

WITNESS THEREFORE THE FOLLOWING AGREEMENT:

Client hereby employs Attorney as legal counsel to represent him/her/they in the above stated matters and issues related to the above-referenced modification action, and any hearings, discovery matters or settlement negotiations of the above-referenced matter and in any related matter necessary to the resolution of any pending controversies.

Client agrees to compensate Attorney by paying attorney's fees at the rate of $[hourly rate] per hour for all legal work performed in this matter. Attorney will charge lesser rates for work performed by legal assistants and/or law clerks [provide rate structure].

Attorney acknowledges the receipt of a pre-paid fee retainer from Client in the amount of $[amount of retainer]. This retainer shall be deposited into the Attorney's trust account, to be drawn out monthly and credited against attorneys fees to be earned by attorney. Any unused retainer shall be refunded to Client if the matter is concluded prior to the exhaustion of any funds held on retainer. No Funds deposited in Attorney's Client trust account will earn interest for Client.

Attorney will provide Client, at monthly intervals, an itemized statement setting forth in reasonable detail, all services by Attorney on behalf of Client, and any costs which have been incurred and/or advanced by Attorney on behalf of Client in the above-referenced matter.

IN THE EVENT AN APPEAL IS NECESSARY AFTER ANY TRIAL, IT IS UNDERSTOOD THAT ATTORNEY WILL NOT PROCEED WITH AN APPEAL WITHOUT AN ADDITIONAL AGREEMENT WITH CLIENT FOR ATTORNEY'S SERVICES.

No claim will be compromised or settled without the express authorization of Client. Client understands that Attorney has made no representations promises or warranties concerning the likelihood of a favorable outcome of any action filed or to be filed. Any statements by Attorney in this regard are statements of opinion only.

Expenses

Client agrees to reimburse Attorney for any and all expenses incurred by Attorney in connection with the prosecution and settlement of claims, including, but not limited to, court costs, deposition fees, transcript fees, reproduction fees, expert witness fees, travel expenses, investigative expenses, telephone expenses and other expenses which Attorney determines to be necessary.

Termination or Withdrawal

In the event Client desires to dismiss Attorney and retain other counsel after the date of signing this contract, IT IS UNDERSTOOD THAT THE TERMS OF THIS CONTRACT PERTAINING TO THE FEES FOR SERVICES RENDERED UP TO AND INCLUDING THE DATE OF DISMISSAL SHALL REMAIN IN FULL FORCE AND EFFECT.

It is agreed that Attorney may withdraw from the Client's representation in this matter at any time if the client insists upon pursuing a course of conduct which, in Attorney's opinion, is illegal or unethical, or is contrary to Attorney's advice even if not illegal, or if Client disregards his obligation to pay for Attorney's fees or expenses when due and payable.

In the event of termination or withdrawal from employment, Attorney will take reasonable steps to avoid foreseeable prejudice to the Client, including giving notice, allowing time for employment of other counsel, and returning to Client all papers and property to which Client is entitled. If Client discharges Attorney, such notice shall be in writing.

This agreement shall be construed under and in accordance with the laws of the State of [State of practice]. All obligations of the parties are performable and fees are to be paid in [your county, and state].

Disposition of Client files and Information

At the conclusion of this matter, Client is advised that all matters in the Client's file shall be returned to Client upon request. Client is further advised to retain all confidential information or original documents from Attorney's file. Client otherwise authorizes Attorney to destroy in a secure manner the information contained in Attorney's file after four years from the date the legal services are completed.

Additional Terms

[Check for local requirements such as Texas' requirement that you advise regarding Grievance Procedures: sample language –

State Bar Rule Notice: Client further has been instructed by Attorney that the Attorney is bound by the Texas Rules of Disciplinary Procedure. Client may contact the State Bar of Texas at www.texasbar.com or toll free at 1-800-932-1900 to obtain information on filing any grievance.]

EXECUTED this_______day of______, 202_.

ATTORNEY:

____

[Name of Attorney/Firm]
[Address]
[Phone number]
[Email address]

CLIENT:

____

[Name of Client]
[Address]
[Phone number]
[Email address]