SAMPLE ADMINISTRATIVE FORM

Please Note: The Florida Information Protection Act (FIPA), [§ 501.171, Fla. Stat.](http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String&URL=0500-0599/0501/Sections/0501.171.html), applies to a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. Personal Information does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable. Please read the applicable law in its entirety to determine when and how notice is required and which agencies, if any, to notify. You may wish to seek legal counsel for further guidance. The Florida Bar cannot provide legal advice.

DATA BREACH NOTIFICATION

[Date]

**IMPORTANT NOTICE TO ALL CLIENTS**

RE: DATA BREACH INCIDENT

Dear Clients:

We are contacting you about a data breach that has occurred at [insert law firm name]. On or about [insert date of incident], [describe *how* the data breach occurred, *what* information may have been taken, and *how* the stolen information may have been misused (if you know)]. Please be assured that all standard protective measures were in place at the time of the incident. Upon discovering the breach, we immediately changed passwords, locks/access codes, and took all affected equipment offline. We have been working alongside our IT specialists to fix any vulnerabilities which may have contributed to the breach.

Our standard practice has been, and remains, to protect all electronic data via password, which changes regularly. Still, there is some degree of risk that your personal, non-public information may have been compromised. The Florida Information Protection Act (FIPA) defines personal information as:

1. An individual's first name or initial and last name in combination with one or more of the following data elements for that individual:
	* A social security number;
	* A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
	* A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;
	* Any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
	* An individual’s health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

([§ 501.171(1)(g)(1), Fla. Stat.](http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String&URL=0500-0599/0501/Sections/0501.171.html))

Generally speaking, we maintain social security numbers for our clients filing bankruptcy or closing real estate transactions. Bankruptcy client information, including social security numbers, was public information prior to December 2003. Since that time, our software has prevented the entire number from printing on the petition, thereby reducing the chance of theft during this data breach. As for our real estate clients, closing files were not typically opened or maintained on the computers that were breached. Therefore, the chance of anyone having obtained your personal, non-public information is small. Nevertheless, we still recommend that you obtain and review your credit report as a precautionary measure. Get your free credit reports from [annualcreditreport.com](http://www.annualcreditreport.com/). Check for any accounts or charges you don’t recognize.

You may wish to notify the three main credit reporting agencies of this incident and require that no accounts be opened or changed in any way without your express written authorization. All three bureaus offer “credit watch” features and offer “three-in-one” reports for your convenience. You can contact the agencies as follows:

Equifax: [equifax.com](http://equifax.com/) or 1-800-525-6285

Experian: [experian.com](http://experian.com/) or 1-888-397-3742

TransUnion: [transunion.com](http://transunion.com/) or 1-800-680-7289

You may also wish to contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You may visit the FTC’s site, [IdentityTheft.gov](https://identitytheft.gov/), for information on appropriate follow-up steps after a breach, depending on the type of personal information that may have been compromised. We have enclosed a copy of [*Identity Theft: A Recovery Plan*](https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf), a comprehensive guide from the FTC to help you guard against and deal with identity theft.

Due to the size of this mailing, please understand that we may not be able to respond to telephone inquiries about the incident. We kindly ask that you forward any comments or questions in writing, and we will respond as quickly as possible.

We sincerely regret having to inform you of this incident and apologize for any inconvenience to you.

Sincerely,

[Lawyer Signature]

[Law Firm Name]