



## ICE (Instant Confidential Exchange) Token

### *“Protecting consumer privacy in payments”*

I am writing about a topic, merchant processing, that you might think is innocuous. You have been told that your merchant processing is compliant. However, does it meet the requirements of state data privacy statutes? Does your current merchant processing contract comply with state laws and/or state common law such as data theft, negligence, and/or invasion of privacy?

Let me give you the lay of the land. As you may have heard, data privacy has become increasingly important. Civil lawsuits are on the rise, and regulators are fining and suing businesses at an ever-increasing pace. At the same time, technology is progressing rapidly to protect the privacy of your patients' data. One vulnerability you may not have considered is merchant processing. Let me explain how it works today and then introduce the technological advance from Fluid Financial, who created the ICE Token.

When a customer, Tom Smith, checks out of Monty's Grocery Store and pays with his credit or debit card, Monty's Grocery Store unknowingly allows Mastercard, Visa, American Express, and/or discover to collect and use that data, revealing that Tom Smith went to Monty's Grocery Store on x date and paid y amount. Up until now, Tom Smith had no way to prevent his credit or debit card company from knowing what services or products he purchased from whom and when.

However, with Fluid's ICE Token, which obtains permission to move the data to the gateway company, the data is de-identified for all parties involved, such as Mastercard, Visa, American Express, Discover, and your bank. What does that mean for Tom Smith? Tom Smith will see on his bank statement, e.g., #2d6j, for \$20.00 on his credit card statement or bank statement. Visa or one of the other card companies will see that symbol, as will the acquiring bank and the merchant processor. The only entity in the process who will know the true purchase of goods or services will be the gateway company, which obtains permission to receive and store the data. Every lawyer will tell you that if data is de-identified, that is the safest course to avoid violating federal or state privacy statutes or running afoul of common law claims of negligence, data theft, or invasion of privacy.

As we know very well, technological advances can change the legal landscape. We urge you to talk to your attorney to find out the cost of analyzing the following issues regarding regulatory liability and/or civil liability, including class actions against your practice for the failure to de-identify your merchant processing transactions. Ask your attorney if they can give you a definitive answer to each issue. Find out the cost to defend you regarding a regulatory fine, a civil lawsuit, or class action lawsuit. Also, inquire about insurance coverage if you are sued on a theory of data theft or invasion of privacy, as well as insurance coverage for fines from a federal or state regulator. Your attorney will not be able to assure you that you have no exposure. They will suggest that you de-identify your customers' data.

#### Question One:

- Does state data privacy law impact me? Is it the law of my state as the doctor, the state of Tom Smith, the gateway company, the state of the merchant processor, the acquiring bank, or the credit or debit card company, or the state of my bank? How much will that analysis cost me? How much will it cost to defend the lawsuit if it is individual or class action? What is the exposure for damages? What is the cost of defending an imposition of a fine? What is the fine exposure for fines?

Question Two:

- What are my duties under my current merchant processing contract? Does either duty under federal law or state data privacy law get imbued into that contract? If so, what does that mean? How much will that analysis cost me? How much will it cost to defend the lawsuit if it is individual or class action? What is the exposure for damages?

Question Three:

- Do I have exposure under a theory of negligence, data theft, and invasion of privacy? Which law applies? Is it the law of my state as the doctor, the state of Tom Smith, the gateway company, the state of the merchant processor, the acquiring bank, or the credit or debit card company, or the state of my bank? How much will that analysis cost me? How much will it cost to defend the lawsuit if it is individual or class action? What is the exposure for damages?

Fluid Financial, who we believe has the only de-identification technology in the United States to both merchant process and be able to de-identify a patient's information/data, offers the same rate you are paying today plus an additional 25 cents per transaction and a monthly fee of \$39.99. Avoid the costs by taking the safest route to avoid fines and civil liability. Switch quickly.

For more information contact

Max Mitchell Newman

PJ21

Email address: [mnhealth2@msn.com](mailto:mnhealth2@msn.com)

Phone 813 380 5700