11

Evans, Sandra E

From: dokgs@yahoo.com
Sent: Wednesday, March 20, 2002 11:45 AM
To: study.comments@ots.treas.gov
Subject: comments on information sharing practices among financial institutions

Dear All;

I would like to share my ideas about this study (of information sharing practices among financial institutions and their affiliates, as required by the Gramm-Leach-Bliley Act of 1999).

I hope that you will find this information useful. And if you do so; please inform me.

I will be very happy to hear that.

Thanks and regards,
D. Oksane Geseli

Financial institutions share consumer "data" among themselves. I used the word "data" instead of "information" because I believe that the difference between the meanings of these 2 words is the main issue to be discussed at the first step.

If we cannot understand, define and explain the "difference" between these 2 words; it will not be possible to answer below questions!

Simply; the "data" is a piece of "information".

If the subject is "information sharing" then sharing the "data" does not mean anything. And unfortunately, we share "the data", not "the information" via existing information sharing systems in the world.

The "data" is the only "element" that we can update or/and change or/and correct; not the information.

Fields, such as name, last name, id number, etc. on a driver licence are the "data" fields (elements) of the driver licence. One of the fields of a driver licence may have "fake data" in it and the other fields may have "correct/real" data. We can share this licence as "fake licence" by using a fraud code pointing out so. But, what about the owner of the licence? Let's assume that he/she is "innocent" and therefore he/she is "the victim". Then we must use a fraud code that will describe the full story (the "information")..

See below scenario:

Let's assume that;

1. One of the members (THE MEMBER) of the credit industry has figured out that a driver licence (DL) used in a credit application is a fake DL (because, for example the number is fake).

2. THE MEMBER created a "fraud record" in its database pointing out that this is a fake DL and sent this record (THE FRAUD RECORD) to the credit bureau. This means that this "information" is now accessable by all other members of the credit bureau because the members can access to this record by performing a search process on the database of th credit bureau.

This means that one of the members (THE MEMBER) let the other members know about the "information" on a fraud case whenever it recognizes a fraudulent transaction.. With another words; THE MEMBER, whenever it recognizes a fraudulent transaction, stores the "data" (information) about a fraud case into a database which is accessable by the other members.
If this is the method of sharing the "information" then it is better not to share the "information"!

Why?

To answer this question let's assume that;

3. The subject DL belongs to a person and this person (THE CUSTOMER) had lost it or it was stolen.

4. The "thief", by changing one of the digits of the number of DL had applied to THE MEMBER for one of the credit products of THE MEMBER and The MEMBER understood that this is a fraudulent application.

5. But, since the "thief" did not (as normal) use THE CUSTOMER's address and telephone number, it is not possible to inform THE CUSTOMER. This means that The CUSTOMER does not know that a "fraud record" on his/her name is being shared.

6. And after a while (may be days or months or even years later) THE CUSTOMER applies to a member (THE MEMBER-X) of the credit industry for a credit product and

6.1. THE MEMBER-X performs a search on the database of the credit bureau.

6.2. THE FRAUD RECORD is reported on the credit report.

What happens then? Here is the real story begins. There are many possibilities:

a. THE MEMBER-X is using an automated application processing system and system rejects the application automatically and THE CUSTOMER does not ask why he/she is rejected. If happens so; then (probably) THE MEMBER-X has lost a good customer and The CUSTOMER lost his/her chance to get the credit!
b. THE MEMBER-X rejects the application and THE CUSTOMER asks "why?" and so; THE CUSTOMER learns the shocking story!

If "a" is the case then there is nothing to say more..

But if "b" is the case then another story begins:

THE CUSTOMER will, for sure, face many problems to prove that he is innocent. Let's assume that THE CUSTOMER made THE MEMBER-X believe that he/she is innocent and DL is his/her stolen DL. This is not enough. Normally, THE CUSTOMER will want THE FRAUD RECORD is being deleted from all databases it is stored. But, this is not easy and also is not a "good" thing to do. If this record is being deleted just to make THE CUSTOMER happy; what will happen if the "thief" is still using this DL to get credit from other members? The other members are in danger! Therefore, "deleting the record" is not a solution.

As you scan imagine that this is a very long and complex story.. It is possible to run it on many other different scenarios.

We all know that the credit industry and the consumers are suffering from fraudulent activities.

* They are losing reputation...

* They are losing good clients and important lifetime relations...
* They are losing money...

Because of many factors, creating an "information sharing system" to detect and stop the FRAUD and/or minimize the risk and cost figures of the FRAUD is not so easy:

The first and the most important factor is the legal factor!
There are, maybe, hundreds of FRAUD types and thousands of combinations of objects used in these fraudulent transactions. It is not easy to create a system to define the category and the objects of a FRAUD clearly and provide such information to be shared between the parties without causing legal problems, misunderstandings and/or wrong interpretations.

The second factor is updating the FRAUD information as soon as it is necessary!
It is very important to update the shared data (information) in the next minute after receiving the last (final/most updated) data & information from a member. Meaning that, in a "reliable" FRAUD Alert System, there is no time to lose to refresh data & information shared.

The third factor is to file the full story (not only the data or the initial information)!
The third factor is to file every single step of the operation cycle and each single "piece of the information" ("data") and therefore let everyone understands what the real story is. Who is who? What is what?

You, as an individual (consumer), are already a victim or for some reason carrying a risk to become a victim:
Someone has used your personal information and you are afraid of suffering from this situation for a long period of your lifetime.
"Because, they say so!"
If the credit industry does not have a system to share the "information" about you to protect your image and credibility then they are right to say so and you are right to be afraid of!

You, as the credit officer in the member organization of the Credit Industry, want to be informed shortly after one of the other members has detected a FRAUD attempt!

* Because it may be associated with one of your "good" clients.
* Because maybe it is associated with one of the accounts in your company's credit portfolio and your company is already a victim.
* Because maybe it is related to one of the credit application records in your company's database and you are about to open an account for it.

You, as the credit officer in the member organization, figured out a FRAUD activity and want to inform the other members.

* Because you need more information and you think that some other members can have what you need.
* Because the information used in the FRAUD belongs to one of your "good clients" and you want to let everyone to know that he/she is innocent and this is an "identity theft case".

It is obvious that the hardest part of implementing a computerized FRAUD System is to create an information sharing technique by which the information about a FRAUD case can be shared among the members (users) without having any difficulties, misunderstandings, wrong interpretations..

Let's assume that there is a very complex FRAUD case and you need to inform other members about it. But, since it is a very complex case you must be very careful with the language or the code that you will use to express the situation.

Are you sure that you will be able to prepare an ALERT MESSAGE that will describe exactly what you want to tell?

May it cause a legal problem if the frame of your sentence in your ALERT MESSAGE is wrong and the person who read this ALERT MESSAGE is misinformed?

Or, let's assume that your ALERT MESSAGE is correct but the FRAUD case is too complex and the person who read this ALERT MESSAGE misunderstood the situation? May this cause a legal problem?

Without rules, a data/information sharing system is more dangerous than not having it all!
A data/information sharing system must have its own principls and rules! Otherwise; you will never know: Who/What is right? Who/What is wrong?

It is possible to create a relational database for each single "story" about a FRAUD case in saBasLanguage.
Here is another "master piece of saBas" that makes saBas really different, much powerful and reliable than other similar systems exist anywhere in the world:

You must access to every single piece of data to express the full story (information) about a fraud case whenever it is necessary by performing a one-shot search.
For many of the FRAUD cases, saying that "this is the story about the FRAUD case and these are the objects used in this story (case)" does not mean that this is the end of the story! You should still be careful and watching out for the future FRAUD attempts that the the same objects are used. And if it happens so; you must add the new (fresh) information to the fraud story.

If the subject is information sharing then the other side of the story is handling the disputes of the consumers on their personal data/information..

The basic question is this:
Do we have a fully automated system for handling the operations and other related services for the complaints and objections of the consumers on their personal information shared (SHARED INFORMATION) among the members of the credit industry?

We all know what the consumers want the members (that sharing consumer data/information among themselves) correct the data/information errors in "hours" (even in "minutes").