Question 1:

The vendors that have their credit card information database stolen/leak should definitely be held liable for their losses whenever their system fails. A vendor’s database is supposed to be very secure since they could be making thousands and millions of credit card transaction a day and with all that information being lost out there, they should be punished for not guarding the information good enough. When a customer is ordering items online and using their personal credit card to do so, they are putting in trust that they will be charged for the amount that they saw, and they are expecting to receive the bought items. The customer does not sign up to have their personal card stolen and maybe even their personal information just because the company’s security is not good enough. With the information out there the hacker could do one of two things, one is to use the card themselves and buy items online and the other is to sell the information to the dark web which in both cases will cost the customer’s money and time to get the issues resolved and maybe get their money back. Depends on the information that was leaked, for example your name, birthdate, and address, it could stay on the internet for a long period of time and no one want that to happen. No matter what, time and money will be wasted just because the vendors did not have good enough security and that’s the reason why they should be punished or at least held liable for the losses.

Question 2:

I believe there is two good options to pick from considering the given situation. Option one is to go with what we got and risk the inadequate security, since it does not contain extreme information, it could be fine to leave it as is. Customer behavior and group affiliations is not as extreme compared to credit card information or passwords. The client would be happy since the project will be finished on time and no additional cost was incurred, but if something bad would happen afterwards, you could expect some bad things. If a breach like such happen, you could expect many complaints and customers wanting their information deleted and to the extreme of being sue with a side of being fired from your job or not being able to find more clients in the future. Option two is to ask for more time and money to upgrade the current security, it would cost a little more and would take longer for the project to finish but the end result will be way better than if it was left alone. The company would be pretty mad at first, but they will most likely understand once you explain to them what the former project manager left on the security side. Most likely no breaches will happen since the security was updated and have a marginally small chance of it happening. All data will be secured and if the upgraded security is good enough, the client can also upgrade their mass data collection to include extreme information in the future if they wished. This would benefit them in a huge way if they want to go that route. I personally would pick route two since it would be the most secure way to proceed with the current project. The pros of upgrading the security outweighs the cost and time that would be saved if you go route one. Not to mention that if a breach did happen and you were the project manager of route one, you could really be expected to be jobless for quite a while.

Citation