Dear leaders and colleagues, when you receive this email, I have already resigned. You receive this email because it might involve the safety of your private information. Please take five minutes to read this letter, thank you. I am Tianbo Song and began to work as an intern in IT department of New York branch in June. Here is the story before I resign in October:

When I came here in June, I was responsible for User Management System (hereinafter referred to as UMS) of debug. UMS contains the office address, telephone, position, email and other personal information of all office staff in North America.

At that time, I asked the department for relevant development documents to understand the system, but there was neither relevant development document nor demand document, because the old framework was out of date and could not be used any more. I proposed to refactor the code and would finish the code refactoring with approval. However, neither the model selection of new framework nor document keeping after refactoring had obtained any approval and reply. I felt worried very much, because in case of no documentation kept for the system involving bank, if the employees’ private information was disclosed because subsequently someone sold off the employees’ information or someone remodified the framework after I left ICBC, I could not stay out of it or assume corresponding responsibilities, and it would also bring unnecessary risks to ICBC. I dared not to further develop any relevant system, and Tony from Risk Department was just recruiting at that time, so I communicated with him and passed the interview. I had planned to do the job of CECL modeling in Risk Department and wait the UMS document arranged by me was approved and filed.

(Explain in technique details within this parenthesis, not need to read if you do not care:

First of all, the financial system should try to avoid using third-party frameworks. If the framework has to used but the development documents, framework selection and code are not reviewed, the consequences of filing will be very serious. Let me give a simple example. The basic function of UMS is based on the organizing and exporting of employee information forms. I can select or publish a framework whose main function is to transmit data and the secondary function is the corresponding function of the form on Github. Due to the lack of authority management of the server by the IT department, if someone uses the ICBC unified administrator account, they can use any desktop in the company and remotely log in to the server where UMS is located. There are dozens of services on the UMS production server, and many people are using the server with their task. Logging in at work makes it more difficult to track records. During my work, I have been asked by an anxious colleague if I have changed the production server. At this time, as long as the malicious framework is used to reconstruct the code and replace the original code, all information can be transmitted to the external server in an open manner while maintaining the function. However, since the main function of the framework is to transmit data, vulnerability scanning cannot classify the server as malicious. In addition, due to the limited space of the departmental backup server, frequent backups may have nowhere to be stored, and the original records will naturally be overwritten. At that time, I requested more than ten phone calls for UMS backup, and the backup was delayed for a week after multi-party coordination. As the last person to rebuild the server with traces, I cannot distinguish the relationship without keeping the development documents and filing, and I will inevitably assume the corresponding responsibilities. At the same time, I will bring unnecessary risks to ICBC.)

On July 9, before the meeting with related personnel from Gamma, I consulted Mr. Guo for the scheme I would submit. I was an intern and really hoped that my scheme could be approved. But Mr. Guo said that he didn’t get along with Frank and Risk Department for a long time, since the problem was proposed by information safety group of Risk Department, we would approve but not help them. At that time, I mentioned my idea of going to Risk Department for modeling in late June. I had a certain professional knowledge, could help the two departments communicate with each other and understand each other, and could share some work to reduce the work pressure of IT Department. Mr. Guo agreed with premise that I could not help Risk Department with communication in remaining more than half a month of working in IT Department (including Tony invited me to assist with relevant database business as IT staff), and Mr. Guo took the initiative to say that I could do my own things.

On July 9, at the meeting with related personnel from Gamma, Mr. Guo thought that I was not tough enough and took over my microphone to say that we would offer no scheme and had no solution even for more time, and they should solve by themselves. But based on the principle of loyalty, I consulted Mr. Guo in the remaining more than half a month and did some tasks of helping colleagues with odd jobs.

On July 19, Mr. Guo suddenly came and angrily told me not to go anywhere but stay in IT Department. I didn’t know what went wrong (because I had no task to do, but just helped colleagues with odd jobs), but then I knew that Mr. Guo had fierce conflict with Frank at the meeting of headquarter.

On July 26, it was supposed to handle my job transfer, I consulted Mr. Guo based on department rules, if he was more emotionally dissatisfied with Frank than last time, I didn’t care waiting for another month and going to Risk Department until the relation between them was eased. But Mr. Guo said directly that it would not happen forever.

Actually, it didn’t matter whether I went to Risk Department or not. In the following few months, I had submitted the documents to Mr. Guo and Mr. Ning who was responsible for development via email, departmental summarization, WeChat and personal meeting for many times but got no approval and filing, and they gave no final suggestions for modification (I had screenshots as evidence, what’s more ridiculous was that when I asked Ms. Ning if she had any past similar development document or demand document for me to reference, she said no and let me to draft by myself). It’s already Oct now, I can’t wait any more, and I have no choice but make this unwise decision, please understand.

I’m writing this email with hope that ICBC attaches more importance to the risk of information safety. I’m not qualified to instruct ICBC headquarter to rectify the atmosphere and build a good mechanism, but I hope ICBC can make efforts to select and use right persons, so that the assigned institutions can show the style of a great bank. Meanwhile, I don’t expect any results brought by this email, but I just hope that related person will think of me in case of similar events.

Wish ICBC better and better!

各位领导，同事，打扰了，当你们收到这封邮件时我应该已经辞职了，您能收到这封邮件是因为有可能涉及到您的隐私信息安全，以下文字将占用您5分钟的阅读时间，请见谅。

我是6月份来纽约分行IT部门实习的宋天博，以下是我10月辞职前发生的故事：

6月我刚来时负责debug 一个名为 ‘User Management system’ 以下简称UMS 的系统，UMS包含北美所有办公人员的办公地址，电话，职务，以及邮件地址等一系列个人信息。

当时我向部门索要相关开发文档想了解一下系统，然而既没有相关的开发文档也没有需求文档，因为旧框架已经过时无法继续使用，我提出重构代码的意见，得到批准后便以最小化原则选择了一个和原来框架相近的框架将代码重构完成。但是，无论从新框架的选型，以及重构后的文档整理，均没有任何评估，和审核，备案。当时我感到十分不解，因为涉及到银行的系统如果没有留任何文档记录，可能会造成严重的风险。

（这里详细说明一下：首先金融系统应该尽量避免使用第三方框架，而如果使用框架却对开发文档，框架选择和代码不审核，备案的后果会非常严重。我举个简单的例子，UMS基本功能是基于员工信息表格的整理和导出，我可以选择或者将一个主要功能为传输数据，次要功能为表格相应功能的框架合法的发布在github上。由于部门对服务器缺乏权限管理，后续如果有人使用ICBC统一的那个管理员账户便可以在公司随意找一个机器再远程登陆UMS所在的服务器，而UMS生产服务器上有数十个服务，很多人都在工作中登录更为追踪记录增加了难度，我在工作中就有过被着急的同事问询是否动过生产服务器的情况。这时只要用恶意框架再重构代码并替换原有代码就可以在保持功能不变的情况下光明正大的传输所有信息到外界的服务器，而由于该框架主要功能就是传输数据，漏洞扫描也无法把这个归类为恶意行为。并且由于部门备份服务器空间有限，经常备份无处可存，原有的记录自然会被覆盖，我当时请求对UMS备份就打了十多通电话并且经过多方协调才延迟了一周进行备份。而作为有迹可查的最后一个重构服务器的人，没有留存开发文档和备案的我既无法撇清关系，也必然承担相应的责任，同时也会给ICBC带来不必要的风险。）

当时我已经不敢再进一步开发任何相关的系统了，当时Risk部门的Tony正在招人，我便和他沟通并且通过了面试，本打算先在风险部进行CECL建模的工作，同时等我整理的UMS文档被批准并存档。

7月9日早上，在和风险部Gamma 相关人员开会前，我先请示了郭总我要提交的服务方案。我是实习的身份，如果真的提了方案希望有人能够审核。怎料郭总却说，他与Frank以及风险部门素来积怨已久，既然是风险部信息安全组提出的问题，那么即使我们给他们的功能下线了也不应该给他们任何帮助。那时我就又重提了我6月底时讲过的想去风险部做模型的想法，我有一定的专业知识，也可以帮助两个部门互相沟通，相互理解，我也可以分担一些工作减轻IT部门的工作压力。郭总虽然同意了，但是条件是我在IT剩下的大半个月不要再到处帮助风险部门对接（当时Tony请我以IT身份帮忙处理相关数据库业务），而且郭总主动提出，我也可以做自己的事。

接着7月9日当天在我和Gamma相关同事开会的时候，看我态度不够强硬，郭总拿过我的话筒，替我直接表明了，我们不给任何方案，再给一些时间也没有任何办法，让她们自己解决。

7月我本可以按照郭总的指示做些自己的事，但是本着忠人之事的原则，我在接下来的大半个月我也请示郭总，做了一些帮助同事打杂的任务。

7月19日郭总突然很气愤的跑过来跟我说哪里也别想去，就留在IT干，我实在不知道我哪里又出现了问题（因为我根本没有任何任务，只是帮助同事打杂），但随后我就了解到郭总似乎又与Frank先生在总行会议上起了激烈的冲突。

7月26日，本应该开始办理我的转岗事宜，我本着所谓的“部门规矩”，请示郭总，如果他比上次情绪上对Frank更加不满，那么我不在意在等一个月，等他们缓和一些我再过去。怎料郭总却直接说，他们永远不会缓解了。

其实去不去风险部并不重要，而我接下来的几个月里多次把我整理好的文档通过邮件，部门总结，微信和面谈的方式给郭总和部门负责开发任务的领导宁总反应需要对UMS提交开发文档并归档，但却迟迟没有批准和存档，也没有最终的修改意见（我有截图作为证据，更离谱的是当我问宁总有没有类似的开发文档哪怕是需求文档可以参考时，却回复说从来都没有，让我自己起草），眼看已经到了10月，我也不能再无休止的等待下去了，为了理清责任，出此下策实属无奈，请大家原谅。

这封邮件只是希望ICBC能够重视起信息安全风险，我更没有资格指点ICBC总行整顿风气、建好机制，在选好人、用好人上下功夫，让外派机构体现大行的风范。同时，我并不期待这封邮件能够导致任何的结果，只是希望通过这封邮件，再有类似的相关事件出现时，相关的人员能够想起我。

塞上纵归他日马，祝愿ICBC越来越好！