



*Summer 2023: Big Data Security and Privacy Protection*

*Course Project, **Due Time, Date** 11:59 PM, September 8, 2023*

Student Name: \_\_\_\_\_ Matriculation Number: \_\_\_\_\_

---

Instructor: Rongxing Lu

The marking scheme is shown in the left margin and [100] constitutes full marks.

Please send your solutions in pdf with name "S23-CP-YourName-StudentID.pdf" to [Xiaoyu.z@zju.edu.cn](mailto:Xiaoyu.z@zju.edu.cn) and [rxlu.cn@gmail.com](mailto:rxlu.cn@gmail.com) before the due date, time (GMT+8). The title of your email is "S23-CP-YourName-StudentID.pdf".

---

- [100] 1. Banks and Financial institutions (FIs) operate in a highly regulated industry. Right at the ideation stage of a product or a project, banks need to keep the risk, compliance, legal, info-security teams in alignment of what they're trying to achieve. Usually, there are processes in place in banks and FIs that vet each product or service before launch; however, in today's world, it's highly critical to pay special attention to checks regarding user data and privacy. Read the following old news (<https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018>), please write down around a 3-page report to identify the possible reasons of the cybersecurity events in the news, and propose your guideline on how to secure financial Big Data including user data in banks and financial institutions. Please describe your guideline as detailed as possible with reasonable justification.

Business

## Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack



BMO and Simplii say thieves stole information, demanded \$1M ransom for safe return

Pete Evans · CBC News · Posted: May 29, 2018 11:25 AM ET | Last Updated: May 30, 2018



Aaron Saltzman reports on victims of a Canadian bank hack. 4:05

### Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack

Pete Evans · CBC News · Posted: May 29, 2018 11:25 AM ET — Last Updated: May 30, 2018

Hackers have threatened to release personal information for nearly 100,000 customers of two Canadian banks unless the lenders pay a \$1-million ransom for its safe return.

On Monday, Bank of Montreal and online bank Simplii Financial owned by CIBC revealed that they learned over the weekend that the identifying personal information of a combined 90,000 different account holders at the two banks was stolen.

'Open banking' holds promise but cybersecurity fears loom for Canadian banks The thieves said they accessed information such as names, account numbers, passwords, security questions and answers, and even social insurance numbers and account balances, by exploiting weaknesses in the two banks' security systems.

"We warned BMO and Simplii that we would share their customers informations if they don't cooperate," a Russian-based email purportedly from the thieves said Monday evening.

How they did it

The email also provided a brief explanation of how they say they hacked the accounts. The hackers claim they were able to gain partial access to accounts by using a common mathematical algorithm designed to quickly validate relatively short numeric sequences such as credit card numbers and social insurance numbers.

The hackers say they used the algorithm to get account numbers, which allowed them to pose as authentic account holders who had simply forgotten their password. They say that was apparently enough to allow them to reset the backup security questions and answers, giving them access to the account.

"They were giving too much permission to half-authenticated account which enabled us to grab all these information," the email said, adding that the bank "was not checking if a password was valid until the security question were input correctly."

The email demanded a ransom of \$1 million in a cryptocurrency known as Ripple be paid for the return of the data by yesterday at midnight, otherwise the information would be released.

"These ... profile will be leaked on fraud forum and fraud community as well as the 90,000 left if we don't get the payment before May 28 2018 11:59PM," the email said.

That deadline has now passed. The cryptocurrency wallet where the hackers ordered the money to be paid was only opened last month, but already has the equivalent of almost \$5 million US in it.

CBC News reached out to both banks for confirmation as to whether any ransom had been paid.

"Our practice is not to make payments to fraudsters," Bank of Montreal said. "We are focused on protecting and helping our customers."

For Simplii's part, the bank said "we are continuing to work with cybersecurity experts, law enforcement and others to protect our Simplii clients' data and interests."

To back up the veracity of their claims, the thieves shared identifying information about two Canadians each a customer of each respective bank.

'Very distressed'

CBC News contacted those two individuals, and both confirmed the veracity of the information the thieves sent out.

"I'm very distressed," one victim told CBC News when told their information had been stolen. "How could this happen? I barely slept last night, I'm so worried."

CBC News has obtained a list circulating online containing personal information of 100 BMO customers, which includes extensive personal information about them, including names, addresses, phone numbers, account numbers, birth dates and Social Insurance Numbers. CBC News has reached out to a number of those individuals, many of whom confirmed the accuracy of the information.

One Simplii customer who was not named in the hackers' email claiming responsibility says he was told by the bank on Monday evening that he, too, is a victim of the hack.

"It's concerning," Mike McCarthy of Edmonton said. "I'm not sure in this day and age what I can do to get control of that data again."

Here's how the FBI says Russian hackers stole Yahoo account secrets "Some of those things you can't change about yourself so I'm sure it's going to exist out there for as long as someone wants to look for it."

McCarthy says he's heartened by the bank's response, offering free credit monitoring and some other services. But he still worries about what he calls "glaring gaps" in the banking system.

"Who knows? Maybe I go back to showing up at the teller," he said. "I don't want to, but who knows what might happen next?"

Bank of Canada warns financial sector vulnerable to cyberattacks