Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Central 1 Credit Union (Organization)
File number	P2017-ND-119 (File #001219)
Date notice received by OIPC	July 17, 2015
Date Organization last provided information	April 24, 2017
Date of decision	August 9, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • names and business email addresses of employees of members of the Organization; • business email addresses of employees of corporate members of financial institutions; and • business email addresses of employees of billers. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information appears to be "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business e-mail address, business fax number and other similar business information."

	Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." In this case, I considered that the disclosure of the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, I find that PIPA applies to the personal information in this case.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On February 19, 2015, while troubleshooting a software issue, an employee of the Organization inadvertently uploaded an Excel file containing the information at issue to the unsecured public area of a website. • The incident was discovered on May 20, 2015, when security staff at two member credit unions informed the Organization that they had discovered an unprotected Excel file accessible on the internet that contained email addresses. Employees whose email addresses were listed in the file had been experiencing an increase in spam. • The Excel file was removed from the website on May 21, 2015.
Affected individuals	The incident affected 7,763 individuals across Canada, including residents of Alberta.
Steps taken to reduce risk of harm to individuals	• The Excel file was removed from the website one day after the breach was discovered, on May 21, 2015. • Reviewed the incident with the employee responsible. • Completed refresher training for employees using the software in question. • Reviewing education program to make any necessary improvements to the guidelines on handling of sensitive data.
Steps taken to notify individuals of the incident	The Organization directly notified its own affected members in Alberta, as well as employees of billers and some corporate members, by email. The Organization also reported that "Of the remaining corporate members, the credit union that has the relationship with the corporate members will notify affected individuals, unless the credit union asks [the Organization] to do so on its behalf.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported that "The most likely type of harm that could result is phishing, specifically spear phishing. This could result in an employee of a credit union or other organization disclosing sensitive business and/or personal information to an unauthorized individual. Organizations may also be subject to increased spam attacks that could contain links to websites with malicious code and/or malware attachments." In my view, the email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	In assessing the likelihood of harm resulting in this case, the Organization reported: *For guidance, Best Buy Canada Ltd., Case File # P2011-ND-01, was referenced. At paragraph 11, the Commissioner sets out a (at least) three prong test for determining whether there is a real risk of significant harm. Based on that test, the potential harm is not considered significant, as the information is not of a sensitive nature and it was exposed accidentally. Additionally:* *- Most organizations already have systems in place to monitor and limit spam and malicious emails.* *- Employees, especially financial institution and corporate employees, are generally aware of the risks of unsolicited emails and emails from unfamiliar senders.* *- In general, a business email address, in association with the employee's name (and other information such as a job title) can be found on publicly-available sources such as the company website, annual report, etc.* I believe the Organization intended to reference Case File #P2011-ND-011, which concerns Best Buy Canada Ltd., rather than Case File #P2011-ND-01, which does not exist and is not posted on my office's website (#P2011-ND-001 is posted but concerns a different organization and circumstances of a breach that are not at all similar to this case).

	In Case File #P2011-ND-011, and particularly at paragraph 11, the former Commissioner said: *Numerous factors are considered when determining whether a real risk of significant harm has occurred, which include but are in no way limited to: the magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether there are indications personal information was misappropriated for nefarious purposes, the sensitivity of the information and the harm that may result.* ***Each breach must be assessed based on the circumstances of that particular case.***[my emphasis] In Case File #P2011-ND-011 the former Commissioner found there was a real risk of significant harm to individuals affected by the incident described, saying "it is not mere speculation, but a reasonable assumption that at some point in the future, the affected … customers will be targeted by spear phishing emails as a result of the … breach." The former Commissioner also said "…a small … portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain personal information. Phishing attempts have been successful in the past and there is no evidence to indicate that the information obtained through the …breach will be treated any differently." Despite the fact many organizations have systems in place to detect malicious emails and, increasingly, individuals may be aware of the possibility of receiving such emails, incidents of phishing occur with regularity as evidenced by the breaches reported to my office. I note further that a significant factor contributing to the former Commissioner's decision in Case File #P2011-ND-011 was the fact that the incident resulted from malicious intent. In this case, there is no malicious incident; instead, the incident resulted from human error. Nonetheless, the information was made available on a public website, and the error was not discovered for almost three months. In my view, these circumstances increase the likelihood of significant harm resulting in this case.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.	

Email addresses could be used to send unsolicited emails and for phishing. Consistent with previous breach notification decisions issued by my office, phishing is a significant harm. Despite the fact many organizations have systems in place to detect malicious emails and, increasingly, individuals may be aware of the possibility of receiving such emails, incidents of phishing occur with regularity as evidenced by the breaches reported to my office. In this case, there is no malicious incident; instead, the incident resulted from human error. Nonetheless, the information was made available on a public website, and the error was not discovered for almost three months. In my view, these circumstances increase the likelihood of significant harm resulting in this case.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand that the Organization directly notified its own affected members in Alberta, as well as employees of billers and some corporate members, by email, and that the credit union that has the relationship with the corporate members notified affected individuals. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner