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	LastPass Technologies Canada ULC (Organization)
Decision number (file number)	P2023-ND-014 (File #028291)
Date notice received by OIPC	December 9, 2022
Date Organization last provided information	March 2, 2023
Date of decision	April 11, 2023
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals whose personal information was collected in Alberta 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 all or some of the following information:
	
	Contents of Unencrypted "Customer Database" including:
	• name,
	• billing address,
	• email address,
	• telephone number,
	• mobile device unique identifier,
	• IP address, and
	• metadata, including:
	  ○ entitlement information (subscription type),
	  ○ number of PBKDF2 SHA256 iterations.
	
	Contents of Unencrypted "Customer Account Secrets" including:
	• multifactor authentication seeds.
	
	Encrypted "Customer Vault Data" including:
	• credentials (usernames and passwords),
	• secure notes, and
	• custom fillable form-field content.

	Unencrypted "Customer Vault Data" including: • certain email addresses, and • website URLs associated with a saved credential. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization's website says it is a provider of "password and identity management solutions." One of the Organization's products / solutions is "a secure digital vault for passwords and login details..." As part of its operations, the Organization "uses Amazon Web Services (AWS) for routine cloud storage, archiving and back up services..." • On November 2, 2022, the Organization was alerted to suspicious activity within its cloud storage environment. • On November 27, 2022, the Organization identified that "there was a sufficient likelihood of customer data being accessed." • On December 15, 2022, the Organization confirmed that a "backup copy of the user main database and encrypted vault data was exfiltrated from the [Organization's] AWS account." • A March 1, 2023 public notice explained "The threat actor was able to copy five of the Binary Large Objects (BLOBs) database shards that were dated: August 20, 2022, August 30, 2022, August 31, 2022, September 8, 2022, and September 16, 2022. This took place between September 8 - 22, 2022." • An investigation determined this incident was the result of a series of cyberattacks that took place in August 2022, in which a threat actor targeted a software engineer and a DevOps engineer. The threat actor ultimately deployed malware on a "DevOps engineer's home computer," leading to the compromise of a "LastPass corporate vault." • "The threat actor then exported the native corporate vault entries and content of shared folders, which contained encrypted secure notes with access and decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups." The attacker "engaged in … enumeration, and exfiltration activities aligned to the cloud storage environment spanning from August 12, 2022 to October 26, 2022."
Affected individuals	The incident affected "approximately 128,000 residents of Alberta."

Steps taken to reduce risk of harm to individuals	• Published online notices regarding the incident. • Engaged external cyber security expertise. • Conducting dark web monitoring to detect disclosure of records. • Enhancing certain administrative and technical safeguards, including improving threat detection and monitoring capability. • Decommissioned affected environments. • Notified law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified of the incident by email on or about November 30, 2022. On December 22, 2022, the Organization published an online public notice with incident updates via their blog. Affected individuals were notified of the online notice by email on December 22, 2022. The Organization published supplemental information about the incident to their blog on March 1, 2023. Affected individuals were notified of the online notice by email on March 1, 2023. The Organization has published statements on social media (Twitter).
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 on December 9, 2022, "individuals may be sent phishing emails." In a December 22, 2022, public notice, the Organization stated: *The threat actor may attempt to use brute force to guess your master password and decrypt the copies of vault data they took … The threat actor may also target customers with phishing attacks, credential stuffing, or other brute force attacks against online accounts associated with your LastPass vault.* In my view, a reasonable person would consider that name, contact information (billing address, email address, telephone number), IP address, mobile device unique identifier, subscription information, and website URLs associated with a saved credential could be used for the purposes of phishing or spear-phishing, increasing affected individuals' vulnerability to identity theft, fraud, and compromise of other online accounts. Brute force or credential stuffing attacks against encrypted vault data or "online accounts associated with [a] LastPass vault" and multifactor authentication seeds could result in the compromise of credentials and unauthorized access to other online accounts.

	Website URLs associated with saved credentials, name, and contact information could be used to cause the harms of embarrassment, hurt or humiliation, and damage to reputation or relationships. The above are all significant harms. It is not clear what information is in individuals' vaults (encrypted secure notes, other custom fillable form-field content); therefore, it is not clear what other possible harms may exist should the encrypted vault data be exposed.
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.	**The Organization's Assessment** With respect to phishing, the Organization assessed the risk as follows: *The likelihood is medium, but the likelihood such [phishing] emails would be effective is low considering notice to individuals.* The Organization's December 22, 2022, blog post assessed attacks against the master password and encrypted vault data and described risk mitigating factors: *[E]ncrypted fields remain secured with 256-bit AES encryption and can only be decrypted with a unique encryption key derived from each user's master password using our Zero Knowledge architecture. As a reminder, the master password is never known to [the Organization] and is not stored or maintained by [the Organization]…* • *Since 2018, [the Organization has] required a twelve-character minimum for master passwords. This greatly minimizes the ability for successful brute force password guessing.* • *To further increase the security of your master password, [the Organization] utilizes a stronger-than-typical implementation of 100,100 iterations of the Password-Based Key Derivation Function (PBKDF2), a password-strengthening algorithm that makes it difficult to guess your master password. You can check the current number of PBKDF2 iterations for your LastPass account here.* • *[The Organization recommends] that you never reuse*

your master password on other websites. If you reuse your master password and that password was ever compromised, a threat actor may use dumps of compromised credentials that are already available on the Internet to attempt to access your account (this is referred to as a "credential stuffing" attack).

If you use the default settings above, it would take millions of years to guess your master password using generally-available password-cracking technology …

However, it is important to note that ***if your master password does not make use of the defaults above, then it would significantly reduce the number of attempts needed to guess it correctly. In this case, as an extra security measure, you should consider minimizing risk by changing passwords of websites you have stored.*** *[all emphasis added]*

Analysis

Unencrypted Customer Database, Customer Vault Data, and Customer Account Secrets

In my view, a reasonable person would consider the likelihood of phishing, spear-phishing, identity theft, fraud, embarrassment, hurt or humiliation, damage to reputation or relationships, and compromise of other online accounts resulting from this incident are increased because personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, deployment of malware, exfiltration of data). The threat actor has downloaded personal information. Further, the threat actor had access to the Organization's system(s) for approximately three months before the incident was contained.

Encrypted Customer Vault Data

The Organization described a number of factors mitigating against the success of possible attacks to the encrypted vault data including:

- the Organization's zero knowledge architecture
- 256-bit AES encryption combined with the use of a stronger-than-typical implementation of 100,100 iterations of the Password-Based Key Derivation Function (PBKDF2), a password-strengthening algorithm (hashing).

I understand that the encrypted vault data "can only be decrypted with a unique encryption key derived from each user's master

	password" and that "it would be extremely difficult to attempt to brute force guess master passwords." However, the Organization recognized that "if your master password does not make use of the defaults above, then it would significantly reduce the number of attempts needed to guess it correctly. In this case, as an extra security measure, you should consider minimizing risk by changing passwords of websites you have stored." The Organization recognized that if users did not use the default settings, the number of attempts needed to guess the master password would be "significantly reduced." The likelihood of harm is connected to and dependent on the affected individual's password hygiene habits and the strength of the master password. The master password can be anywhere on the spectrum from very strong (using completely random passwords) to very weak, human generated passwords. The Organization did not require a minimum strength of a master password until 2018 (twelve-character minimum with additional complexity requirements). This, in my view, increases the likelihood of harm for those affected individuals. The Organization also notes "Make sure all members of your Families account follow these best practices. The safety of your shared items is determined by the person with the weakest master password." The Organization published a technical whitepaper explaining that vault encryption keys are strengthened by PBKDF2 hashing. The level of protection from brute force attacks varies with the number of PBKDF2 iterations applied. The protection afforded by this hashing scheme, however, is also connected to the strength of an affected individual's master password. The March 1, 2023, public update stated that the number of PBKDF2 iterations applied to accounts was exfiltrated as part of the metadata. This information, in addition to the master password salts (email address) are in the custody of the threat actor. The fact that the threat actor has this knowledge is a factor increasing the likelihood of harm as it affects the protection offered by this strengthening algorithm against brute force attacks. The security bulletin recommends customers raise the default minimum iterations to 600,000. Prior to this, the default was 100,100. The Organization has recommended customers evaluate and consider changing their master passwords, set their master password hash iteration to at least 600,000, evaluate the passwords

	stored in the vault for strength, and ensure they are using the multifactor authentication on the Organization's account and other important accounts. It is recommending the affected individuals take many steps to better protect themselves "against potential brute force attacks." The Organization states in the security bulletin that the reason the Organization created the guide is to "help you confirm that you are following our best practices and respond to the recent LastPass security incident in a way that meets your personal needs." In my view, a reasonable person would consider that the likelihood of harm resulting from the exfiltration of customer vault data is increased, by way of possible brute force and or credential stuffing attacks, where individuals' master passwords are 'weak,' easily guessable using generally-available technology, re-used elsewhere, or are otherwise compromised in another incident. The number of PBKDF2 iterations applied to accounts was exfiltrated by the threat actor. This information, in addition to the master password salts (email address) are in the custody of the threat actor. All these factors increase the likelihood of harm. While the Organization has provided affected individuals with guidance on how to decrease the likelihood of harm by taking certain steps with respect to their account, the decrease of the likelihood of harm is dependent on the user taking these steps. In addition, the encrypted vaults are in the custody of the threat actor. The threat actor may have had custody of the vaults since September 8, 2022. This factor increases the likelihood of harm. A lack of evidence that personal information in encrypted vaults has been misused does not mitigate against future harm as brute force attacks and decryption of vault data could occur any time after the breach.
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. Name, contact information (billing address, email address, telephone number), IP address, mobile device unique identifier, subscription information, and website URLs associated with a saved credential could be used for the purposes of phishing or spear-phishing, increasing affected individuals' vulnerability to identity theft, fraud, and compromise of other online accounts. Brute force or credential stuffing attacks against encrypted vault data or "online accounts associated with [a] LastPass vault" and multifactor authentication seeds could result in the compromise of	

credentials and unauthorized access to other online accounts.Website URLs associated with saved credentials, name, and contact information could be used to cause the harms of embarrassment, hurt or humiliation, and damage to reputation or relationships.

The above are all significant harms.

It is not clear what information is in individuals' vaults (encrypted secure notes, other custom fillable form-field content); thus it is not clear what other possible harms may exist should the encrypted vault data be exposed.

The likelihood of phishing, spear-phishing, identity theft, fraud, embarrassment, hurt or humiliation, damage to reputation or relationships, and compromise of other online accounts resulting from this incident are increased because personal information was compromised due to the malicious action of a threat actor (deliberate intrusion, deployment of malware, exfiltration of data). The threat actor has downloaded personal information. Further, the threat actor had access to the Organization's system(s) for approximately three months before the incident was contained.

The likelihood of harm resulting from the exfiltration of customer vault data is increased, by way of possible brute force and or credential stuffing attacks, where individuals' master passwords are 'weak,' easily guessable using generally-available technology, re-used elsewhere, or are otherwise compromised in another incident.

The number of PBKDF2 iterations applied to accounts was exfiltrated by the threat actor. This information, in addition to the master password salts (email address) are in the custody of the threat actor. All these factors increase the likelihood of harm.

While the Organization has provided affected individuals with guidance on how to decrease the likelihood of harm by taking certain steps with respect to their account, the decrease of the likelihood of harm is dependent on the user taking these steps.

In addition, the encrypted vaults are in the custody of the threat actor. The threat actor may have had custody of the vaults since September 8, 2022. This factor increases the likelihood of harm.

A lack of evidence that personal information in encrypted vaults has been misused does not mitigate against future harm as brute force attacks and decryption of vault data could occur any time after the breach.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

The Organization said it notified affected individuals by email on or about November 30, 2022. This email contained some of the information required under section 19.1 of the Regulation, however, it did not contain a description of the personal information involved (s.19.1(b)(iii)) or contact information for a person who can answer questions about the unauthorized access (s.19.1(1)(v)) as required by the Regulation.

The Organization emailed affected individuals again on December 22, 2022, directing individuals to an

updated online blog post “with important information about [the] ongoing investigation.” The December 22, 2022, notice and online blog post also did not meet the requirements of the Regulation as described above.

On or about March 1, 2023, an email notification was sent to affected individuals. The email notice contained a link to an updated blog post that contained information of “new findings and important information, including what happened and the actions we have taken, what data was accessed, what we have done to secure LastPass, actions we are recommending customers take to protect themselves or their businesses, and what you can expect from us going forward.”

I accept that the email notification sent to affected individuals on or about March 1, 2023, meets the requirements of the s. 19.1 of the Regulation. The blog link in the email notice contains a detailed description of customer data affected by the incident. A link was also included to a security bulletin that includes contact information for the Organization. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance