Additional 16681

Appendix -- Sample Template of Notice to Individuals

Notice of Data Incident

Dear (user first name/last name),

What Happened

At approximately 1:45 a.m. on Saturday, March 14, 2020, The Jamaica National Group experienced a data breach as a result of a ransomware attack.

What Information was Involved

Although our services are now substantially back online, we have identified that data relating to some members and customers was possibly taken during the data security incident. However, our investigations have found that some of your information would have been accessible to an unauthorised third party, therefore, it is possible, albeit unlikely, that you could be amongst those whose personal data was taken.

The information relating to you that may have been taken, may be information that is required to open an account with JN Bank, such as:

- The name and branch at which you opened an account
- The type of account that you opened
- Your personal customer information form
- Proof of address
- Proof of employment
- Copy identification documents
- Copy birth certificate
- Character reference details

There is also the possibility that for some customers credit card details could have been compromised.

What We Are Doing

We have already taken several steps in response to the incident. As required by law, we have advised the regulatory agencies in all countries in which we operate. Additionally, we have:

- Notified the Police and security agencies locally and overseas
- Advised relevant banks

- Advised our credit card supplier, which is doing enhanced monitoring of credit card transactions
- Undertaken a complete review of our IT systems to further strengthen our infrastructure
- Appointed a specialist IT security and forensic provider to investigate the incident
- Implemented a special email address **wecare@jngroup.com** to support customers who may have queries. Customers may also call **876-968-5096; 876-960-5508**
- Established a process to help customers through this period, which could include credit remediation and identity protection services, such as LifeLock and Identity Force for a period of 12 months.

What you can do

We have no evidence that the data that may have been taken was targeted or has been misused. However, we think this kind of incident needs to be treated with caution. Given the nature of this information, it is important that we make you aware of the incident and any associated risks.

There is a risk that the data that may have been extracted from our network could be used to attempt to facilitate fraud, identity theft or social engineering attempts. As a result, we recommend that you exercise increased vigilance in all matters relating to your personal and/or business details over the next 12-24 months, and report suspected identity theft incidents to JN Bank, law enforcement including your Attorney General, and the Federal Trade Commission.

To assist, we are able to offer 12 months of credit and identity monitoring at no cost through a leading credit monitoring service provider. Please let us know if you are interested, and we will send you the information and activation codes that you will need to set it up.

If you would like to institute a fraud alert and/or security freeze at no charge, you may contact the major credit agencies. The credit agencies may be contacted as follows:

TransUnion	P.O. Box 1000 Chester, PA 19022	1-800-916-8800
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241	1-800-685-1111
Experian	P.O. Box 2104 Allen, TX 75013-0949	1-888-397-3742

For further information on fraud alerts and security freezes, you may contact the Federal Trade Commission. The Federal Trade Commission's website is https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-

security/advice-consumers, its address is 600 Pennsylvania Avenue, NW, Washington, DC 20580, and its telephone number is 1-877-382-4357.

You have the right to obtain a police report concerning the data breach.

It may also be prudent for you to obtain replacement identity documents. We would suggest that you contact your local issuing authority and follow their advice.

In addition, it is good practice to:

- Check that all details for direct debits are up to date, and delete any that are no longer needed;
- Check bank accounts regularly and contact the bank if you see any transactions you do not recognise. If the transaction relates to a bank account that you hold with us, please contact **876-968-5096; 876-960-5508 or by emailing wecare@jngroup.com**
- Be suspicious if anyone contacts you by email, phone call or text message asking you to confirm your personal details;
- Enable two-factor authentication on all of your online services that offer this;
- Use different passwords for different online accounts.

For More Information

If you have any questions, then please don't hesitate to reply to this email or contact us at **876-968-5096; 876-960-5508 or by emailing wecare@jngroup.com**. We will be happy to help you in any way we can.

We are sincerely sorry for any concern and inconvenience this may have caused you. We would like to reassure you that we take our responsibilities for the protection of your data very seriously.

Supplemental Notice of Data Incident

Dear (user first name/last name),

What Happened

As you are aware, on March 14, 2020, The Jamaica National Group experienced a data breach as a result of a ransomware attack. We would like to update you regarding this breach.

What Information Was Involved

Our continuing investigation revealed that some of your data was acquired and made available to others online. As we currently understand it, this includes the following categories of information (not all of which may be current): [CATEGORIES FROM SPREADSHEET].

There is a risk that this data could be used to attempt to facilitate fraud, identity theft or social engineering attempts.

What We Are Doing

We have continued to investigate the breach. As required by law, we have advised the regulatory agencies in all countries in which we operate. Additionally, we have:

- Notified the Police and security agencies locally and overseas
- Advised relevant banks
- Advised our credit card supplier, which is doing enhanced monitoring of credit card transactions
- Undertaken a complete review of our IT systems to further strengthen our infrastructure
- Appointed a specialist IT security and forensic provider to investigate the incident
- Implemented a special email address **wecare@jngroup.com** to support customers who may have queries. Customers may also call **876-968-5096; 876-960-5508**
- Established a process to help customers through this period, which could include credit remediation and identity protection services, such as LifeLock and Identity Force for a period of 12 months.

What You Can Do

We strongly reiterate the recommendations in our prior notice:

We recommend that you exercise increased vigilance in all matters relating to your personal and/or business details over the next 12-24 months, and report suspected identity theft incidents to JN Bank, law enforcement including your Attorney General, and the Federal Trade Commission.

To assist, we are able to offer 12 months of credit and identity monitoring at no cost through a leading credit monitoring service provider. Please let us know if you are interested, and we will send you the information and activation codes that you will need to set it up.

If you would like to institute a fraud alert and/or security freeze at no charge, you may contact the major credit agencies. The credit agencies may be contacted as follows:

TransUnion	P.O. Box 1000 Chester, PA 19022	1-800-916-8800
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241	1-800-685-1111
Experian	P.O. Box 2104 Allen, TX 75013-0949	1-888-397-3742

For further information on fraud alerts and security freezes, you may contact the Federal Trade Commission. The Federal Trade Commission's website is https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/advice-consumers, its address is 600 Pennsylvania Avenue, NW, Washington, DC 20580, and its telephone number is 1-877-382-4357.

You have the right to obtain a police report concerning the data breach.

It may also be prudent for you to obtain replacement identity documents. We would suggest that you contact your local issuing authority and follow their advice.

In addition, it is good practice to:

- Check that all details for direct debits are up to date, and delete any that are no longer needed;
- Check bank accounts regularly and contact the bank if you see any transactions you do not recognize. If the transaction relates to a bank account that you hold with us, please contact **876-968-5096; 876-960-5508 or by emailing wecare@jngroup.com**
- Be suspicious if anyone contacts you by email, phone call or text message asking you to confirm your personal details;
- Enable two-factor authentication on all of your online services that offer this;
- Use different passwords for different online accounts.

For More Information

If you have any questions, then please don't hesitate to reply to this email or contact us at **876-968-5096; 876-960-5508 or by emailing wecare@jngroup.com**. We will be happy to help you in any way we can.

We are sincerely sorry for any concern and inconvenience this may have caused you. We would like to reassure you that we take our responsibilities for the protection of your data very seriously.