HINSHAW

ATTORNEYS AT LAW
One California Street, 18th Floor
San Francisco, CA. 94111

415-362-6000
415-834-9070 (fax)
www.hinshawlaw.com

Erik M. Kowalewsky
415-263-8135
ekowalewsky@hinshawlaw.com

March 30, 2020

VIA ELECTRONIC MAIL

New Hampshire Bank Commissioner
New Hampshire Banking Department
53 Regional Drive, Suite 200
Concord NH 03301
nhbd@banking.nh.gov

Re: JN Group - Notice of Breach of Consumer Information

To Whom It May Concern:

We represent Jamaica National Group Limited and Jamaica National Bank (together "JNB") and on JNB's behalf, we are writing to notify you of a data breach that has affected JNB's customers. JNB, a banking services provider, is located at

JN Bank
2-4 Constant Spring Road
Kingston 10, Jamaica

Synopsis Of The Incident

On Saturday March 14, at approximately 1:45 am, JNB discovered that many of its core systems had been encrypted as a result of a ransomware cyber-attack. This attack was an intrusion into JNB's servers, and encryption of the system files and certain back-up files rendering the systems inoperable. This meant that employees had no access to the banking system, which resulted in an inability to process any transactions or use the email service. Essentially, JNB was shut down; however, Phoenix, the Bank's core banking system, was unaffected.

The outbreak was initially detected in the Jamaica office, then subsequently in the Florida office. The perpetrators left a ransom note, and provided a web-based contact portal to engage with and communicate their ransom demands. The ransom demanded was approximately US$5.5MM in Monero cryptocurrency, and the attackers indicated that the ransom would be increased to US$10MM after 6 days (March 20). If the funds were not paid within that specified time, customer data would be exposed on the internet.

The matter was immediately reported to the Bank of Jamaica, the local regulatory body for the bank, and thereafter, consistent updates have been provided.

On March 17 and 18, JNB received private messages via its social media page and phone calls to its Contact Centre. The messages were believed to be from the perpetrators, who threatened to publish customers' data if the ransom was not paid or contact made with them. Given that the bank maintains full backups of its data on tape, it was determined that there was no need to pay the ransom to recover the data.

The type of ransomware at issue is Sodinokibi, a description of which can be found at https://www.acronis.com/en-us/articles/sodinokibi-ransomware/. This malware is associated with the REvil hacker group.

At present, the volume of exfiltrated data is unknown; however, JNB has identified that personal data relating to some customers was taken during the data security incident. This information included what is required to open an account with JNB, such as:

- The name and branch at which customers opened an account
- The type of account that was opened
- 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.

Actions Taken In Response

JNB's Board of Directors has been kept apprised of the incident via ongoing correspondence and board meetings.

JNB appointed a specialist IT security and forensic provider, Storm Guidance, to investigate the incident. Technical investigations are still being conducted, including to determine the entry vector. At this time, the compromise is believed to have happened via a malicious phishing email sent to a staff member in the Florida office.

JNB contacted its local and international insurance broker and provider, MGI Brokers and Howden (UK), who initiated their cyber-crime response team of forensic cyber-crimes professionals, lawyers and communications experts. Meetings are being held daily with the JNB IT and cyber-security teams to get a full understanding of the nature and scope of the attack.

JNB has been able to gradually restore its systems from backup tapes in a secure offline (sterile) environment. It is in the process of updating transactions conducted on March 13, 2020. It is taking several necessary precautions to ensure that the recovery process is comprehensive and that no malware is carried over. It created a new domain, changed all administrator passwords and

undertook a complete review of IT systems to tighten the security and further strengthen infrastructure.

JNB contacted the Jamaican Commissioner of Police who assigned the case to a team from the Major Organised Crime and Anti-Corruption Agency (MOCA). MOCA has begun its investigation and is coordinating with the National Crime Agency (UK) which, in turn, advised US Secret Service. These agencies are trying to identify the origins of the attack and to assess JNB's network for safety.

JNB is communicating with the agencies responsible for data protection in the United Kingdom and The Cayman Islands as the law requires the reporting of any data breach which could result in the exposure of personal data. It is also communicating with regulators and others as required by law, in Jamaica, Canada, the Cayman Islands and the United States (of which this letter is part).

JNB has been communicating with its members and customers about the incident since March 14, 2020, and has notified all potentially affected customers (a template for this notification to Florida residents is below, in the Appendix).

Number of Individuals in New Hampshire

At this time, JNB believes that 23 customers in New Hampshire could have been impacted by the security breach. Notice was given to customers on March 20, 2020 via electronic mail.

Services Being or Scheduled to be Offered to Residents and Instructions

JNB advised its credit card supplier, which is conducting enhanced monitoring of credit card transactions.

JNB 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.** JNB has also established a process to help customers through this period, which include credit monitoring and remediation, and identity protection services such as LifeLock and Identity Force for a period of 12 months, at no cost to the customer.

JNB is also providing a fraud alert and/or security freeze, at no charge, to enable customers to contact the major credit agencies, TransUnion, Equifax and Experian. Customers were advised to contact the Federal Trade Commission to obtain further information on fraud alerts and security freezes at https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security/advice-consumers.

Next Steps

1. Work toward full restoration of all services.
2. Continued investigations by local and international security agencies.
3. Preparation of a comprehensive report to regulators and Board of Directors on completion of the technical investigations, which are still ongoing.
4. Continued communication with all stakeholders.

JNB has already put in place a wide range of measures to prevent this happening again and will be undertaking a further review with more improvements very soon. Security is an ongoing process and it is prioritized.

Contact Information for Further Information

Should you have any questions, or require further information, please contact me as set forth above, or on my mobile phone, 1-415-786-7333.

Sincerely,

HINSHAW & CULBERTSON LLP

Erik M. Kowalewsky

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.