NWL®
INSURANCE COMPANY

Dear Valued Agent:

National Western Life Insurance Company ("NWL") was the victim of a malware incident impacting certain company systems. NWL conducted a thorough investigation, with the assistance of third-party forensic specialists, and learned that certain data had been accessed and/or acquired by an unauthorized actor. On December 21, 2020, NWL confirmed that personal information related to certain individuals was included in the impacted data. These impacted individuals include parties to life insurance or annuity policies as well as agents. NWL is providing notice of this incident to potentially impacted individuals, including agents and/or agent's clients who may receive a notice. This notice describes the event and provides steps that individuals can take to protect their sensitive information. It also includes an offer of credit monitoring at NWL's expense.

We have prepared the below Frequently Asked Questions to help your team respond to potential questions from agents and policyholders who received this notice. If your clients have additional questions regarding this event, please direct those clients to the dedicated toll-free call center established specifically for this event at 1-800-599-9658. This call center will be operational beginning on Monday January 25, 2021.

We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we notified federal law enforcement and are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

National Western Life Insurance Company ("NWL") - Frequently Asked Questions

1. **What happened?**
   On August 15, 2020, NWL discovered a malware incident impacting certain company systems

2. **When did NWL learn of this incident?**
   NWL discovered the malware incident on August 15, 2020, and confirmed the identities of potentially affected individuals on December 21, 2020.

3. **Am I affected?**
   NWL is sending written notice of this incident to individuals identified to date as potentially affected by the incident.

4. **What type of information was potentially accessed?**
   The type(s) of information potentially accessed varies by individual, and the letters sent to the impacted individuals states the exact type(s) of information that was impacted.

5. **Does NWL know who is responsible for this?**
   NWL has not identified the specific individual or individuals who are responsible for this event, although the investigation confirmed that the unauthorized individuals were not associated with NWL. We reported this event to law enforcement.

6. **What is NWL doing to prevent this from happening again?**
   NWL takes this incident and the security of personal information in its care very seriously. Upon learning of this incident, NWL moved quickly to investigate and respond, assess the security of its systems, restore functionality to its environment, and notify potentially affected individuals. As part of NWL's ongoing commitment to the security of information, NWL notified federal law enforcement and is reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event.

7. **Is NWL offering any type of monitoring services to affected individuals?**
   NWL is offering impacted individuals with access to free credit-monitoring and identity restoration services through CyberScout. The letter sent to impacted individuals contains information about the services and instructions on how to enroll to receive them.

8. **What can I do to advise my clients to protect against identity theft or fraud?**
   Steps an individual can take to protect against identity theft and fraud include the following:

   - **Monitoring your financial statements carefully.**
   - **Monitoring your credit reports for suspicious or unauthorized activity.**
   - **Placing a fraud alert on your credit file.** You have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file
   - **Placing a security freeze on your credit file.** A security freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent.
   - **Contacting the Federal Trade Commission and your state Attorney General** to learn more about identity theft, fraud alerts, security freezes, and other steps you can take to protect yourself. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261.
   - **Reporting incidents of suspected or actual identity theft or fraud** to law enforcement, the Federal Trade Commission, and your state Attorney General.

9. **What is the purpose of a "fraud alert"?**
   An initial fraud alert is a 1-year alert that is placed on a consumer's credit file at no cost to the consumer. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit.

10. **What is the purpose of a "security freeze"?**
    A security freeze will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent.

11. **Should impacted individuals check their credit report?**
    You should monitor your credit report regardless of whether your information has been exposed or you think you may be a victim of identity theft or fraud. Every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling toll-free, 1-877-322-8228.

12. **If someone thinks may be the victim of identity theft, what should they do?**
    If you or someone else believes they are a victim of attempted or actual identity theft or fraud, we encourage them to take the following steps:

    - Contact your financial institution to protect or close any accounts that may have been tampered with or opened fraudulently.
    - Contact the credit reporting agencies to place a "fraud alert" or a "credit freeze" on your credit reports.
    - File a police report and ask for a copy for your records.
    - File a complaint that you have been a victim of identity theft with the Federal Trade Commission at https://www.identitytheft.gov/.
    - File a complaint that you have been a victim of identity theft with your state attorney general.
    - Keep good records.
        - **o** Keep notes of anyone you talk to regarding this incident, what s/he told you, and the date of the conversation;
        - **o** Keep originals of all correspondence or forms relating to the suspicious activity, identity theft, or fraud; and
        - **o** Retain originals of supporting documentation, such as police reports and letters to and from creditors; send copies only.
    - Keep old files, even if you believe the problem is resolved.

13. **Should impacted individuals report this to law enforcement?**
    If you believe you are or may be the victim of identity theft or fraud, NWL encourages you to file a report with law enforcement.

14. **How do those impacted by this data incident activate their complimentary protection services?**
    The enrollment instructions can be found in the notice letter that was mailed to those impacted.

15. **What can I do to protect myself?**
    While NWL is unaware of any actual misuse of impacted individuals' information, we encourage you to better protect against identity theft and fraud if you feel it is appropriate to do so by taking the steps included in our letter.

16. **Is the letter I received legitimate?**
    Yes, NWL worked with a third-party vendor to print and mail the letter you received. It is legitimate.

NWL®
INSURANCE COMPANY

512-836-1010
800-922-9422

nationalwesternlife.com
mynwl.com

10801 N Mopac Expy, Bldg. 3
Austin, TX 78759-5415

PO Box 209080
Austin, TX 78720-9080