

May 7, 2021

Via Mail

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
Phone: (603) 271-3643

Re: Data Security Event: Public-Facing Web Quotes

RECEIVED  
MAY 10 2021  
CONSUMER PROTECTION

Dear Deputy Attorney General Young,

Noblr Risk Management, LLC as attorney-in-fact for Noblr Reciprocal Exchange (“Noblr”) is submitting this notice to provide the New Hampshire Attorney General with information regarding a suspected cybersecurity event involving unauthorized access to consumer personal information (“PI”) pursuant to N.H. Rev. Stat. § 359-C:20.

Noblr maintains a public-facing website that includes an instant quote feature. Recent irregularities in traffic flow to our instant quote feature suggest that Noblr may have been the target of the type of cyber fraud attack referenced in Cyber Fraud Alert issued by the NY DFS on February 16, 2021 (“the Fraud Alert”).<sup>1</sup>

On January 21, 2021, Noblr’s web team noticed unusual quote activity consisting of a spike in unfinished quotes through its instant quote webpage. Noblr immediately launched an internal investigation. The initial investigation revealed that these quotes may have been initiated by both individual actors and automatic means (aka “a Bot”) and appeared intended to scrape driver’s license numbers from the website that were inadvertently included in unredacted form in the page source code. During the instant quote process, the user is required to enter personal data (name and date of birth) into the quoting system. Noblr then supplements this information on the backend with additional related information about that individual and in some cases other household drivers, including driver’s license information, pulled from Verisk Analytics and matched to the information submitted by the user to provide a quote. Attackers could also have gone through the entire quote process to access driver’s license numbers from the final policy application documents provided after obtaining a quote.

On January 25, 2021, following the initial discovery of unusual quote activity, Noblr’s security team began blocking suspicious IP addresses. On January 27, 2021, when Noblr’s security team determined that the attackers were able to access unredacted driver’s licenses, Noblr altered its instant quote system in order to mask all driver’s license numbers in the source code and in the final application page. As a result, the attackers were no longer able to obtain driver’s license numbers via their attacks. Additionally, throughout this period Noblr’s security team took action to constantly revise rate limit thresholds on its quote page adjusting to traffic patterns to combat these attacks.

As an additional security measure, on February 12, 2021, Noblr’s security team began masking additional information returned from Verisk Analytics, including dates of birth and vehicle identification numbers, in the source code and insurance application page.

The information involved is:

- Full Name;

---

<sup>1</sup> The Fraud Alert is available at [https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/il20210216\\_cyber\\_fraud\\_alert](https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert).

- Address; and
- Driver's License Number

Noblr has completed its investigation to determine the scope of impact of this incident, including identifying individuals who may have been affected and their states of residence. On February 23, 2021 Noblr determined that the affected individuals included New Hampshire residents. While Noblr is unable to determine whether all potentially affected individuals actually had personal information affected, Noblr is erring on the side of being over-inclusive in determining who may have been affected. Based on our investigation, Noblr believes at least 65 New Hampshire residents were affected by the incident. Noblr plans to mail individual notifications by May 14, 2021, which will provide free identity theft protection services. Noblr also intends to notify consumer reporting agencies.

If you have any questions or require additional information, please contact me directly by phone at [REDACTED]

Cordially,

[REDACTED]

May 7, 2021

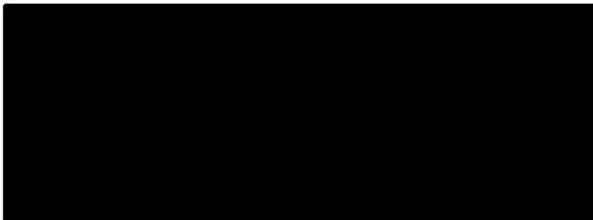
Via Mail

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
Phone: (603) 271-3643  
Re: Data Security Event: Public-Facing Web Quotes

Dear Deputy Attorney General Young,

When posting the notice of the cybersecurity incident to the Office's public website, please use the attached, redacted version of the notice to avoid public posting of the contact information for the Chief Legal Officer of Noblr.

Cordially,



May 7, 2021

Via Mail

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301  
Phone: (603) 271-3643  
Re: Data Security Event: Public-Facing Web Quotes

Dear Deputy Attorney General Young,

Nobl Risk Management, LLC as attorney-in-fact for Noblr Reciprocal Exchange ("Noblr") is submitting this notice to provide the New Hampshire Attorney General with information regarding a suspected cybersecurity event involving unauthorized access to consumer personal information ("PI") pursuant to N.H. Rev. Stat. § 359-C:20.

Noblr maintains a public-facing website that includes an instant quote feature. Recent irregularities in traffic flow to our instant quote feature suggest that Noblr may have been the target of the type of cyber fraud attack referenced in Cyber Fraud Alert issued by the NY DFS on February 16, 2021 ("the Fraud Alert").<sup>1</sup>

On January 21, 2021, Noblr's web team noticed unusual quote activity consisting of a spike in unfinished quotes through its instant quote webpage. Noblr immediately launched an internal investigation. The initial investigation revealed that these quotes may have been initiated by both individual actors and automatic means (aka "a Bot") and appeared intended to scrape driver's license numbers from the website that were inadvertently included in unredacted form in the page source code. During the instant quote process, the user is required to enter personal data (name and date of birth) into the quoting system. Noblr then supplements this information on the backend with additional related information about that individual and in some cases other household drivers, including driver's license information, pulled from Verisk Analytics and matched to the information submitted by the user to provide a quote. Attackers could also have gone through the entire quote process to access driver's license numbers from the final policy application documents provided after obtaining a quote.

On January 25, 2021, following the initial discovery of unusual quote activity, Noblr's security team began blocking suspicious IP addresses. On January 27, 2021, when Noblr's security team determined that the attackers were able to access unredacted driver's licenses, Noblr altered its instant quote system in order to mask all driver's license numbers in the source code and in the final application page. As a result, the attackers were no longer able to obtain driver's license numbers via their attacks. Additionally, throughout this period Noblr's security team took action to constantly revise rate limit thresholds on its quote page adjusting to traffic patterns to combat these attacks.

As an additional security measure, on February 12, 2021, Noblr's security team began masking additional information returned from Verisk Analytics, including dates of birth and vehicle identification numbers, in the source code and insurance application page.

The information involved is:

- Full Name;

---

<sup>1</sup> The Fraud Alert is available at [https://www.dfs.ny.gov/industry\\_guidance/industry\\_letters/ll20210216\\_cyber\\_fraud\\_alert](https://www.dfs.ny.gov/industry_guidance/industry_letters/ll20210216_cyber_fraud_alert).

- Address; and
- Driver's License Number

Noblr has completed its investigation to determine the scope of impact of this incident, including identifying individuals who may have been affected and their states of residence. On February 23, 2021 Noblr determined that the affected individuals included New Hampshire residents. While Noblr is unable to determine whether all potentially affected individuals actually had personal information affected, Noblr is erring on the side of being over-inclusive in determining who may have been affected. Based on our investigation, Noblr believes at least 65 New Hampshire residents were affected by the incident. Noblr plans to mail individual notifications by May 14, 2021, which will provide free identity theft protection services. Noblr also intends to notify consumer reporting agencies.

If you have any questions or require additional information, please contact me directly by phone at [REDACTED] or by email at [REDACTED]

Cordially,

[REDACTED]  
Chief Legal Officer