HINSHAW

Alerts

New York State Department of Financial Services Warns of New Fraudulent Campaign Targeting Consumer NPI

February 23, 2021
Hinshaw Privacy & Cyber Bytes

On February 16, the New York State Department of Financial Services (DFS) issued a cyber fraud alert, warning of a growing cybercriminal campaign to steal consumer, Nonpublic Information (NPI). The hacked data is being taken from public-facing websites and used to obtain pandemic and unemployment benefits. The first reports of fraud were received in late December 2020, and early January 2021, from automobile insurers, who reported that cybercriminals were stealing unredacted driver's license numbers by hacking their websites' instant insurance premium quote function.

The attacks target public-facing websites that display or transmit consumer NPI, and some hackers have even obtained fully redacted information. Thus far, affected entities have been primarily automobile insurers with "Instant Quote Websites," although any entity with a consumer-facing website utilizing instant quotes is at risk.

Some of the methods used to illegally obtain NPI include:

- Taking unredacted NPI from websites' Hypertext Markup Language (HTML)
- Using developer debug tools to intercept and decode unredacted NPI
- Manipulating website NPI-redaction technology to fully reveal the information

DFS recommends that its regulated entities use data analytics and website traffic metrics to identify suspicious activity such as an unusual number of abandoned quotes in a short time frame or submissions that are terminated as soon as NPI is revealed. Other recommended strategies to prevent attacks include:

- Reviewing website security controls and browser web developer tool functionality;
- Properly implementing and ensuring redaction and data obfuscation for NPI throughout the entirety of NPI transmission;
- Confirming privacy protections are up to date;
- Reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides;

Service Areas

Privacy, Security & Artificial Intelligence

- Scrubbing public code repositories for proprietary code;
- Blocking IP addresses of suspected unauthorized users; and
- Implementing a quote limit per user session.

In light of recent hacks and the unprecedented surge in benefits fraud seen during the COVID-19 pandemic, DFS recommends that entities refrain from displaying any NPI, even if redacted, to users on public-facing websites unless there is a "compelling reason" to do so.

DFS-regulated entities should identify and resolve any cybersecurity flaws immediately. If an attack does occur, it must be reported pursuant to 23 NYCRR Section 500.17(a) as soon as possible, but within 72 hours at the latest.

Related Content

- Heather McArn Discusses Warnings by NYS DFS of 'Widespread" Data Breach Cybercrime Campaign