

# New York State Intelligence Center

## Cyber Intelligence Bulletin



CAU@nysic.ny.gov  
1-866-48-NYSIC (866-486-9742)

July 6, 2020

NYSIC-CYB-20-05

**ATTN:** All Partners

**SUBJECT:** Criminals Exploit COVID-19 to Commit Unemployment Fraud

**OVERVIEW:** The New York State Intelligence Center (NYSIC) Cyber Analysis Unit (CAU) is providing the following information for your situational awareness. Local, State, and Federal law enforcement are currently investigating a widespread fraud campaign in which victims' identities are being used to file false unemployment claims. This fraud campaign is likely capitalizing on the surge of unemployment claims relating to the current COVID-19 pandemic and has affected both the private and public sector. Victims, who have not filed unemployment claims, have received notifications from their employer's Human Resources (HR) department, or the New York State Department of Labor (DOL), indicating an unemployment claim has been filed on their behalf.

**RECOMMENDATIONS:** The NYSIC CAU recommends that the following steps be considered for individuals who are a victim of employment fraud.


- Step One – Contact Human Resources
  - Contact your organization's HR staff to coordinate and report the incident to your employer.
- Step Two – Contact New York State Department of Labor
  - Report the fraud to New York State DOL at 1-888-598-2077 or through their online form: <https://labor.ny.gov/agencyinfo/uifraud.shtm>
    - You will need the following information for identity verification:
      - Social Security Number (SSN)
      - Address
      - Phone Number
      - Email address
      - Information on how you learned a claim was filed on your behalf, when the fraud began, and whether the fraud is ongoing.
- Step Three – File a Police Report
  - File an online or non-emergency report with the agency whose jurisdiction you live in.

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.

## UNCLASSIFIED

- Step Four – Report to the Three Major Credit Bureaus
  - Obtain your free credit report from Equifax, Experian, and TransUnion at <https://www.annualcreditreport.com> or call 1-877-322-8228.
  - Report to the credit bureaus that a fraudulent claim was made using your identity and provide them with the case number from your police report. You can have a fraud alert put on your identity and/or freeze your credit. Either can be done free of charge.
    - A fraud alert will make it more difficult for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That bureau will then notify the other two credit bureaus.
    - Experian: 1-888-397-3742
    - TransUnion: 1-800-680-7289
    - Equifax: 1-888-766-0008
  - Check your credit activity at least once a year. As a victim of identity theft, you have the right to check it monthly if you choose.
  - If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for more protection. You can accomplish this by visiting <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.
- Step Five – Federal Trade Commission (FTC) & Internal Revenue Service (IRS)
  - File a short report with the FTC at <https://www.identitytheft.gov>. Provide the case number from your police report. Additional information can be found at <https://www.ftc.gov/idtheft>.
- Step Six – Keep Your Notes
  - Retain any notes, copies of emails, etc., related to your reports and the fraud activity. You can reference them if you face any identity issues or locate inaccuracies on your credit history sometime in the future.

### **ACTIONS TO FURTHER PROTECT YOUR IDENTITY:**

- Services that lock credit information can help, though you must provide companies with your own personal data, potentially creating more risk.
-  Attached to this bulletin, for your convenience, is a previously disseminated joint product between the NYSIC and the National Capital Region Threat Intelligence Consortium (NTIC). The product, titled (TLP: WHITE) Doxing Mitigation Guide, serves as an easy reference to help individuals remove their personal information from public records websites. Click on the thumbtack icon to access. In addition, there are many helpful websites that will walk you through the process of securing your own data. You can search “how to do opt-outs and credit freeze” or use some of the third-party resources below:

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.

## UNCLASSIFIED

- (U) <https://ssd.eff.org/en> – The Electronic Frontier Foundation has several guides for privacy and security.
- (U) <https://www.nytimes.com/wirecutter/reviews/best-password-managers/> – Get a password manager. Most fraud is committed using data obtained from previous internet breaches of hotel chains, entertainment services, and other widely-used digital productivity tools. That is why it is important to never use the same password twice.
- (U) <https://authy.com/guides> – Use multi-factor authentication (a secondary security code) on your most important accounts.
- Most importantly, be vigilant and watch out for things like phishing emails, vishing fraud calls, and mail/package theft which can lead to your identity being compromised.
- Be wary of free applications and offers which could be mining your data.

### **ADDITIONAL RESOURCES:**

- (U) <https://www.tripwire.com/state-of-security/security-data-protection/guide-digital-privacy-yourfamily>
- (U) <https://protonmail.com/blog/coronavirus-email-scams>
- (U) <https://lifehacker.com/s/dataprivacy>
- (U) <https://www.digitaltrends.com/computing/how-to-increase-your-privacy-security-zoom>
- (U) <https://www.consumer.ftc.gov/blog/2020/03/online-security-tips-working-home>

For further information regarding the content of this bulletin, please contact the NYSIC CAU at (518) 786-2191 or [CAU@nysic.ny.gov](mailto:CAU@nysic.ny.gov).

Please note that some of this information describes first amendment protected activities. The NYSIC recognizes that Americans have constitutionally protected rights to assemble, speak, and petition the government. The NYSIC safeguards these rights and only reports on First Amendment protected activities, although no violence or criminality has been observed, this information is provided for operational planning in the interest of assuring the safety and security of the demonstrators and the public.

Requirements: NY-SIN- 1.3, 1.4, 1.8

UNCLASSIFIED