CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0114

UNEMPLOYMENT FRAUD IN THE CRIMINAL UNDERGROUND

Recorded Future®

This report reviews the current threat landscape of unemployment fraud in the United States within closed sources and underground reporting. It contains information gathered using the Recorded Future® Platform, as well as additional open source intelligence (OSINT), dark web sources, and underground forum research. It will be of interest to organizations seeking to better understand unemployment fraud within the criminal underground, as well as investigators of threat actors performing such attacks.

Executive Summary

The COVID-19 pandemic has led to the commoditization of a variety of criminal services themed around unemployment relief originally meant to be distributed to those whose lives have been disrupted by the virus. Unemployment fraud has become increasingly accessible to threat actors lately and presents a low barrier of entry for fledgling cybercriminals. The success of fraud campaigns this year themed around relief efforts to combat the COVID-19 pandemic is likely the result of a combination of factors, including successful social engineering campaigns, the use of money mules operating throughout the U.S., and threat actors' use of login information or personally identifiable information (PII) exposed during data breaches, dumps, or leaks. Some fraudsters targeting unemployment benefit systems are more likely to rely on traditional forms of social engineering such as targeted phishing emails directed at a company's executive leadership. Other tactics, such as the suspected use of money mules in connection with this fraudulent activity, overlap with the tactics of other cybercriminal groups that specialize in various types of fraud, particularly crews that specialize in business email compromise (BEC) schemes.

Given the volume of underground references to the sale of unemployment fraud tutorials and the number of views these methods generate, many fraudsters are likely still new at conducting this form of fraud. Recorded Future has seen no evidence to suspect that actors are exploiting vulnerabilities within government systems, relying instead on their ability to opportunistically target as many victims around the country as possible by harvesting previously exposed information. The general increase in unemployment fraud throughout 2020 was also likely compounded by gaps in the security hygiene of multiple government organizations responsible for safeguarding unemployment applicant data both virtually and physically. This is evidenced by actors in some states believed to be attempting to intercept physical mail that contained personal information tied to unemployment claims. The general flood of fraudulent unemployment requests that has overwhelmed government workers in many states is also enabled by the low barrier to entry for cybercriminals who can purchase stolen accounts or cheap tutorials and methods on how they can conduct similar fraud.

Key Judgments and Findings

- The promotion of fraudulent unemployment services within closed-source reporting over the past six months can be divided into two broad categories:
    - The sale of tutorials or methods to file fraudulent claims
    - The sale of direct access to unemployment relief accounts that often contain a pre-existing balance of funds
- Over the past six months, cybercriminals have demonstrated a preference to advertise unemployment fraud tutorials or services via messaging platforms over criminal forums, shops, or marketplaces, specifically Telegram.
- Underground sources promoting unemployment fraud services typically specialize in a variety of other forms of fraud simultaneously, including credit card fraud and tax fraud.
- The scale of fraudulent unemployment claims within the U.S. has become widespread enough in recent months to unlikely be attributed to a single threat entity.

- Open source reporting on the reported losses stemming from unemployment fraud activity assessed to be in the millions of dollars has very likely contributed to the growing level of interest among underground threat actors.
- Money mules likely remain a critical component of the unemployment fraud supply chain as evidenced by images uploaded by underground sellers of fraudulent unemployment methods and open source reports surrounding the arrests of suspected mules throughout 2020.

Background

Since the onset of the COVID-19 pandemic, rampant unemployment fraud has been reported throughout the U.S., with every state being impacted to varying degrees. This has manifested in various forms, from threat actors filing unemployment claims using stolen PII to state officials contending with reports of money mules funneling stolen funds to fraudulent threat actors operating overseas.

- In January 2020, the Federal Bureau of Investigation (FBI) detailed how cybercriminals use spoofed websites to harvest PII and steal money to conduct fake hiring scams with increasing complexity, advertising alongside legitimate employers and job placement firms to target victims of all skill and income levels. Criminals seeking PII to conduct unemployment fraud are likely to continue to harvest information from previously reported data dumps or breaches or within other criminal marketplaces, often automated, that sell the information at low costs.
- Four months later, the U.S. Secret Service (USSS) linked increasing reports of fraud targeting state unemployment insurance programs to a "well-organized" Nigerian fraud ring. Researchers with Agari published information that attributed a portion of this Nigerian fraud occurring at the time to a group of cybercriminals dubbed Scattered Canary. Potential losses as a result of the group's activities over the past several years are assessed to be in the hundreds of millions of dollars. The USSS said the fraud network is believed to include hundreds of money mules, a term used to describe willing or unwitting individuals who are recruited to help launder the proceeds of fraudulent financial transactions.

Reports of rampant unemployment fraud continue to persist across multiple states. Recorded Future has seen no instances of unemployment fraud that have resulted from an inherent vulnerability within any government systems; rather, reports have detailed various techniques used by individual fraudsters from state to state, making it unlikely that all reports of unemployment fraud that have emerged this year are due to one overarching threat entity. The general increase in unemployment fraud throughout 2020 was likely compounded by failures in the security hygiene of multiple government organizations responsible for safeguarding unemployment applicant data. Security experts believe multiple states likely had pre-existing issues related to their ability to combat this specific form of fraud even prior to the COVID-19 pandemic, including failures to:

- Implement or renew identity verification software to review claims before they are disseminated
- Cross-check benefit claims against personal data on other individuals such as prison inmates, individuals listed as deceased, or out-of-state residents
- Ensure that applicant PII such as Social Security numbers (SSN) are not included in mail correspondence susceptible to physical theft

It is very likely that emerging cybercriminals have become emboldened by open source reports detailing how easy it is to conduct this form of fraudulent activity with no prior knowledge of unemployment systems, combined with the relatively low price of purchasing a tutorial or method to facilitate their activities.

Threat Analysis

The promotion of fraudulent unemployment services within closed source reporting over the past six months can be divided into two broad categories:

- The sale of tutorials or methods to file fraudulent claims with government systems or platforms that assist with unemployment relief
- The sale of direct access to unemployment relief accounts that often contain a pre-existing balance of funds

In March 2020, U.S. lawmakers passed the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which established the Pandemic Unemployment Assistance (PUA) program. This program expands unemployment insurance eligibility to self-employed workers, freelancers, independent contractors, and part-time workers impacted by the coronavirus. Though the PUA program is only one component of unemployment relief offered by government entities within the U.S. in response to the pandemic, it has continued to be an integral component of the growing volume of underground advertisements linked to unemployment fraud.

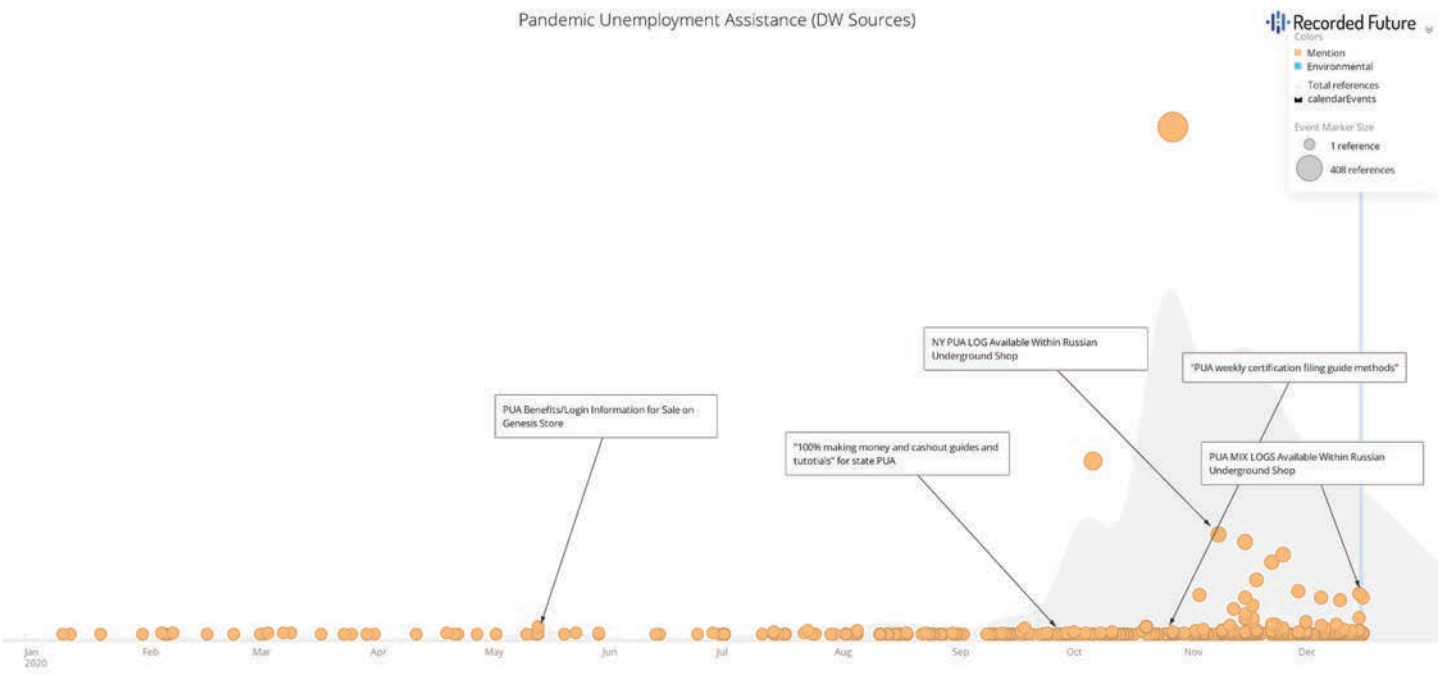

Figure 1: PUA program mentions within dark web sources (Source: Recorded Future)

The visual below shows the results of a survey provided to members of one Telegram channel devoted to multiple forms of fraudulent activity. Though the sale of PUA information came in last place in the survey, its very inclusion on the survey demonstrates that this element of fraudulent activity has generated enough demand among cybercriminals to warrant its own sales category within closed sources. Recorded Future has knowledge of at least one Telegram channel implementing an "operation" as a result of expectations that provisions surrounding unemployment relief were set to expire at the end of 2020, making fraudulent PUA claims a priority for admins of the channel attempting to generate as much revenue as possible in the event that the PUA program or other unemployment relief offerings were suddenly to cease.

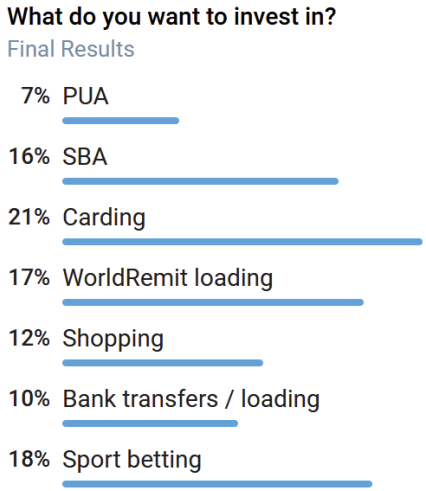

Figure 2: November 2020 survey in Telegram channel dedicated to fraud activities (Source: Telegram)

Over the past six months, cybercriminals have demonstrated a preference for advertising unemployment fraud tutorials or account information via messaging platforms over criminal forums, shops, or marketplaces. However, the demand within traditional marketplaces remains high enough for administrators to continue to support various offerings related to unemployment fraud.

Another appealing aspect of this form of fraud is the relatively low price of tutorials or account information. Recorded Future observed tutorials and methods related to conducting unemployment fraud selling for anywhere between $5 to $100, depending on the state being targeted. The price of PUA information or access to a state government platform containing a pre-existing balance of relief funds was typically higher (as denoted in Figure 3 below, where some threat actors were asking for between $80 to $100 for PUA information associated with New York and Wisconsin unemployment claims).

Threat actors selling this information demonstrated a willingness to forgo accounts with relief balances valued in the thousands of dollars to ensure the long-term success of their underground business model. Additionally, the higher price for direct access to accounts with pre-existing balances as opposed to the tutorials is likely a result of buyers being in the position to more easily access the funds that another veteran actor likely already procured. This is in contrast with tutorials where the buyer is still ultimately responsible for obtaining victim accounts to achieve profit while avoiding attention from law enforcement.

Other fraud methods related to unemployment scams contained what cybercriminals considered to be useful tips to increase the likelihood of achieving success when submitting a fraudulent claim. Tips recommended by fraudsters across multiple tutorials included the following:

- If asked on an application as to when the COVID-19 pandemic affected your employment activities, put March 25, 2020, just two days prior to when the CARES Act was implemented by Congress.
- Filing a claim as "Self-Employed" when possible will net applicants more money than those who filed that they work for another company.
    - This same guide later advised other fraudsters which job they had success with when filing claims. In this tutorial's case, the author recommended pretending to be a "professional photographer" or another job that would be more difficult to fulfill within a remote environment.
- If asked about how much you earned annually in 2019, when filing a fraudulent claim, list an amount between $16,850 and $42,100. The author in this case likely believed that providing a salary above a particular threshold would increase the likelihood of it being flagged by law enforcement investigators or state officials reviewing individual claims.
- Social engineering techniques were also encouraged within multiple tutorials. In one guide, the authors reported that calling a PUA "claim line" and entering a Social Security number (SSN) obtained from another source would verify whether that individual already had an open unemployment relief claim. If no claim had been filed yet, public record aggregation websites such as Verified and Truthfinder were recommended as sources of additional PII on a target. The actors specifically advised using "good" SSN and date of birth (DOB) information on a target to conduct further research on these public record aggregation sites, likely in an attempt to harvest additional PII. However, the actors also showed a level of bias within this guide, with their final recommendation being to visit a specific underground marketplace they are affiliated with to purchase additional information.

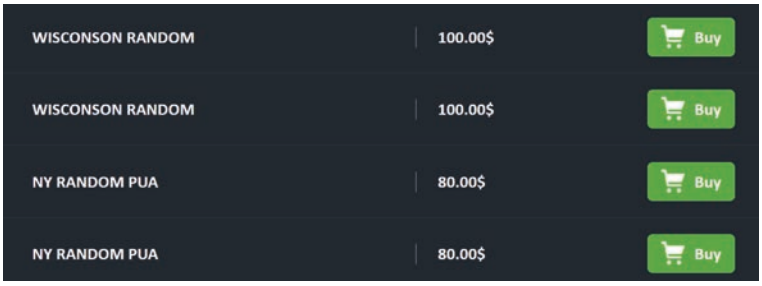

Figure 3: Sale of access to "random" PUA account information

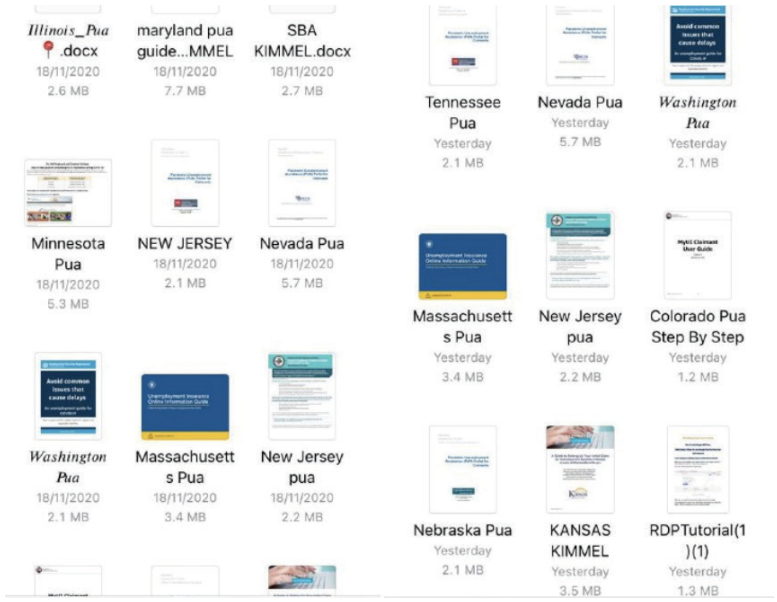

Figure 4: Screenshot of state PUA offerings from a single underground actor (Source: Telegram)

Underground sources selling fraudulent unemployment relief tutorials or account information typically specialize in other forms of fraud, including credit card and tax fraud. Additionally, sellers of these types of fraud do not appear to devote all resources to targeting unemployment systems in one state at a time. Instead, they offer services to access information from a variety of states simultaneously, based on client demand and the level of difficulty in obtaining access to unemployment relief accounts within a particular state.

Criminal shops such as Genesis Store and Russian Market that specialize in the sale of an end user's browsing history or "digital footprint" have also regularly contained login information for state government domains associated with unemployment relief throughout 2020. Recorded Future saw no indication or comments among cybercriminals that these "bots" containing state government login information were being specifically purchased to commit acts of unemployment fraud, though the lack of a discussion functionality within these shops make it difficult to determine the specific motivation behind purchases from these sources.

Alert to Changes in Government Monitoring

As a result of the steady uptick in reports of unemployment fraud across the U.S., states have attempted to mitigate the threat posed by this form of fraudulent activity to varying degrees. As of November 2020, the USSS reported 700 open investigations related to fraud targeting the Paycheck Protection Program and the Unemployment Relief Insurance program. As individual states continue to develop stronger security postures to combat this rampant fraud, cybercriminals advertising unemployment fraud methods or account information are continuing to monitor these changes as well and adjusting accordingly.

- Figure 5 below shows an administrator of a Telegram channel devoted to fraud activity advising members to avoid purchasing or attempting to access unemployment platforms linked to seven specific U.S. states they no longer believed to be distributing financial relief.
- Individual Telegram channels appear to have varying recommendations as to which state is or is not an ideal target at any given time. For example, within two weeks of the Telegram post in Figure 5, originally uploaded in November 2020, threat actors resumed selling methods or account information associated with state systems in Ohio within the same channel, despite these prior warnings by channel administrators.
- Threat actors within these messaging platform channels have also expressed concern that some states are more capable of identifying their location than others. In one scenario, Recorded Future observed a comment from a user advising users to stay away from four specific U.S. states they believed to be likely using tracking applications to monitor for fraudulent claims. The use of proxy IP addresses were highly encouraged within closed sources to prevent this form of tracking and ensuring that a user is not locked out of any unemployment platforms, were government entities to flag their originating IP address as suspicious.

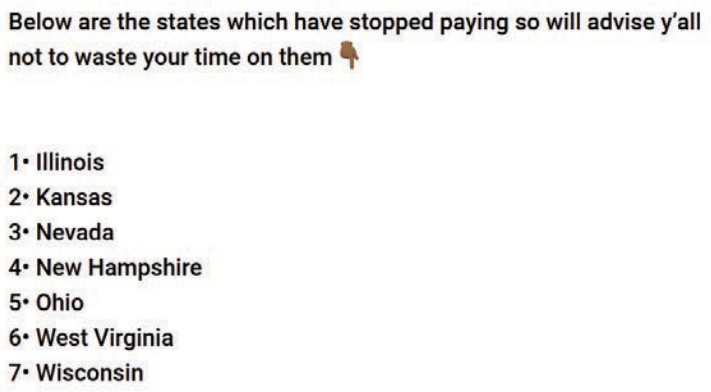

Figure 5: Threat actor advising channel members to avoid targeting certain states (Source: Telegram)

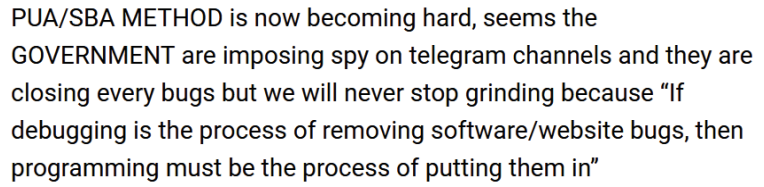

Figure 6: Warning from admin about government efforts to spy on Telegram channels (Source: Telegram)

We are not aware of any security vulnerabilities within government or corporate systems that have assisted in the spread of this fraudulent activity. It is more likely that threat actors will continue to opportunistically target unemployment relief platforms by harvesting exposed login information or purchasing bundles of PII for sale within underground sources.

Assisting Other Fraudsters

Generally, administrators maintaining channels within messaging platforms devoted to unemployment fraud were receptive to the idea of mentoring newer users, likely in an attempt to develop a long-term relationship with partners capable of generating demand for their channels and increasing revenue. This willingness among cybercriminals to partner with one another on unemployment fraud carried over to cybercriminal forums as well, where we observed recurring requests from users seeking "serious" partners for long term-fraud activity. Given that these threads encouraged interested parties to contact the vendor via private channels, the visibility Recorded Future has had into the potential success of these partnerships has been limited.

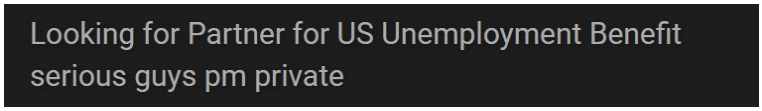

Figure 7: Request for unemployment benefit partner

Vendors of employment scams or PUA fraud methods are often involved in several different scams simultaneously, including disaster relief fraud, Social Security fraud, tax fraud, and credit card fraud. This is the norm for cybercriminal organizations able to operate multiple services capable of providing different streams of revenue.

Recorded Future reviewed several tutorials and methods circulating within the criminal underground regarding a combination of PUA or general unemployment fraud techniques. For the majority of the methods advertised, cybercriminals were expected to already be in possession of stolen PII or "fullz" to take advantage of the guides and be in a position to turn a profit. Fullz is a slang term for "full information" that criminals who steal PII use to refer to a set of information on a prospective fraud

victim, generally including an individual's name, address, date of birth, Social Security and driver's license numbers, as well as the PII of family members and any other miscellaneous information available (such as criminal or employment records).

The same sellers of PUA fraud methods were very often willing to sell this information separately at additional cost. This demonstrates that financial success remains the underlying motivation, despite any attempts by the vendors to portray themselves as good Samaritans willing to assist fledgling criminals who may be new to this type of fraudulent activity.

Unemployment Fraud Targeting and Attribution

In May 2020, researchers at the security firm Agari published their findings regarding a Nigerian cybercriminal group tracked as "Scattered Canary" committing fraudulent unemployment and CARES Act claims throughout the U.S. The Scattered Canary cybercriminal group acts as a full-service business email compromise (BEC) operation that uses scams, such as email impersonation and phishing, to manipulate businesses into paying phony contracts and other fake invoices. Based on Agari's telemetry, most of the targets were located in seven U.S. states: Florida, Massachusetts, North Carolina, Oklahoma, Rhode Island, Washington, and Wyoming. Threat actors associated with Scattered Canary were reported to have used a combination of prepaid cards to receive payments and mass-create email accounts:

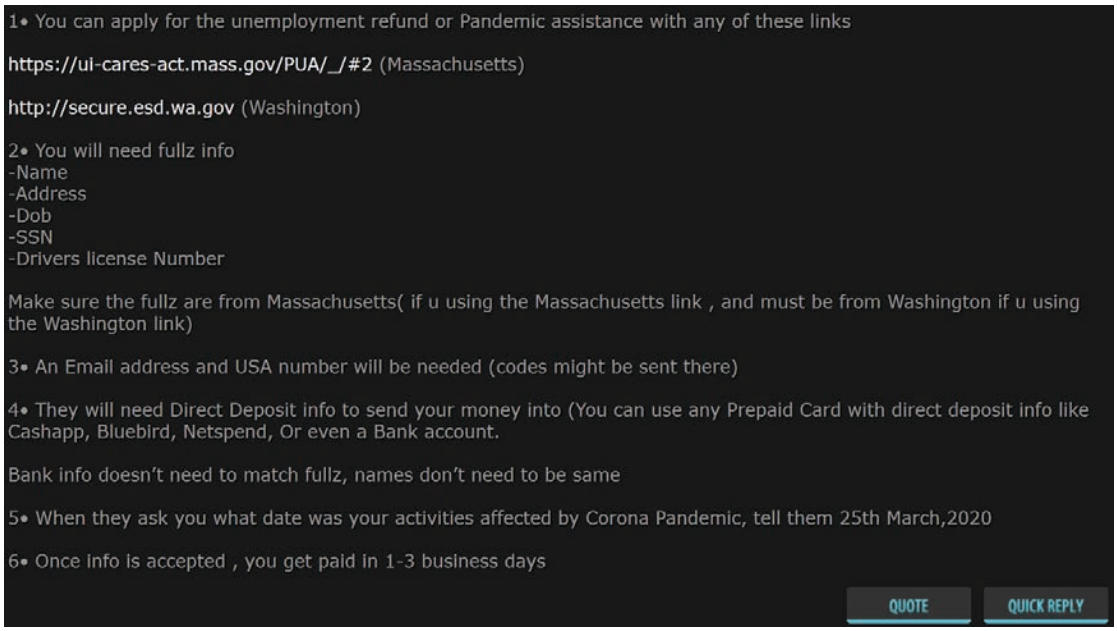

Figure 8: Underground forum member discussing how to apply for fraudulent claims in Washington and Massachusetts

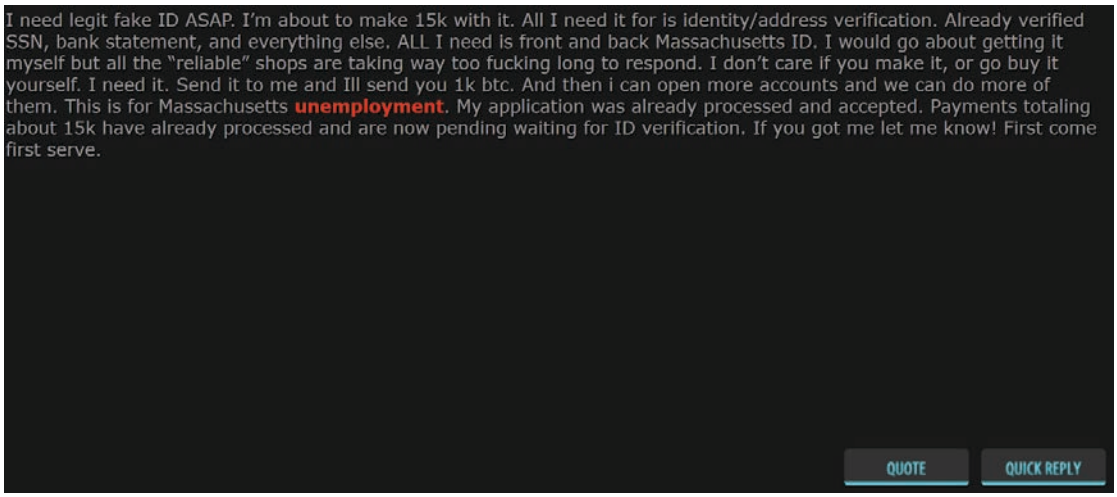

Figure 9: Underground member requesting a fake ID to commit Massachusetts unemployment fraud

- Overall, Scattered Canary used at least 47 prepaid card accounts from Green Dot to receive the fraudulent payments.
- Scattered Canary used Gmail accounts to mass-create accounts on each target website. Because Google ignores periods when interpreting Gmail addresses, Scattered Canary is believed to have been able to create dozens of accounts on state unemployment websites and the IRS website dedicated to processing CARES Act payments for non-tax filers (freefilefillableforms[.]com).
    - Examples of the Gmail dot formatting structure used by Scattered Canary to send unemployment assistance phishing emails:
        - badactor2021@gmail[.]com
        - badactor202.1@gmail[.]com
        - badactor202.21@gmail[.]com

By using this tactic, Scattered Canary was able to scale their operations more efficiently by directing all communications to a single Gmail account. According to Agari, this removes the need to create and monitor a new email account for every account they create on a website, ultimately making transactions faster and more efficient.

The targeting of state unemployment benefits was reported by Agari to be of interest to the group, which had specifically targeted Texas unemployment systems under nine identities as of May 2020. At this time, Recorded Future does not have further insight into how many of the fraudulent claims linked to Scattered Canary are being paid out by the individual states. However, a review of videos uploaded to messaging platforms selling state unemployment relief information did reveal a likely nexus to operators based in West Africa.

- One video uploaded to a fraud messaging platform revealed a likely member of the channel receiving a package from Samamiah (Shipping) Enterprise Limited, a shipping and delivery company that accepts goods for carriage (door-to-door) from the U.K. to Ghana. According to Agari, 10 percent of BEC fraud originated from Ghana between May 2019 and July 2020.

Victim reports obtained by Recorded Future state that the requesters typically knew a target's name, SSN, and place of employment, but all the other data is static. In some scenarios reported to Recorded Future, requesters know the target's name, SSN, and place of employment, likely attempting to target executives or individuals of high networth. This is a common technique within BEC campaigns orchestrated by threat entities like Scattered Canary, which was first identified by Agari as a result of the threat entity impersonating an executive at Agari in an email targeting their chief financial officer.

Fraudulent unemployment claims within the U.S. are widespread enough that they are unlikely coming from a single threat entity. Threat actors have likely become emboldened by open source reports of the monetary impact that fraudulent unemployment claims continue to have.

Though this reporting focuses specifically on unemployment fraud circulating within closed source reporting, some opportunistic actors with little regard to maintaining operational security have also been observed advertising on traditional social media platforms. The large volume of open source reporting on the subject of unemployment fraud activity and losses estimated to be in the millions has very likely contributed to the growing level of interest and motivation among underground threat actors.

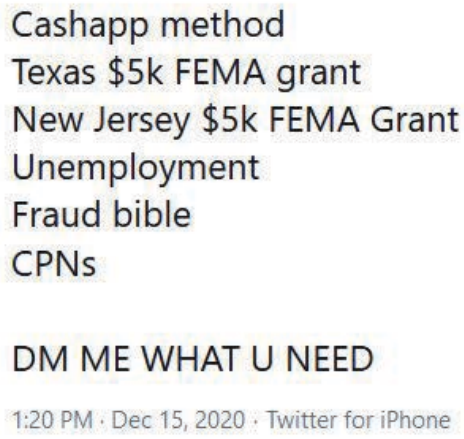

Figure 10: Social media ad for unemployment methods/tutorials

This level of interest has been reflected in multiple statistics reported across both the state and local levels of government since the start of December 2020.

- A follow-up investigation by KrebsOnSecurity in August 2020 reconfirmed that a group of scammers was likely sharing highly detailed personal and financial records of Americans via a free email service. Another undisclosed source informed KrebsOnSecurity that they had been monitoring the group's communications for several weeks and sharing the information with U.S. state and federal authorities in a bid to disrupt their fraudulent activity. Similar to earlier reports on the scale of these unemployment fraud campaigns, the source said the threat group appears to consist of several hundred individuals who collectively have stolen tens of millions of dollars from U.S. state and federal treasuries via phony loan applications with the U.S. Small Business Administration (SBA) and through fraudulent unemployment insurance claims made against several U.S. states.

  - This nexus to phony loan applications filed with the U.S. SBA is noteworthy given that it overlaps with the techniques of Scattered Canary operations detailed by Agari in May 2020.
- In a warning to state legislators in December 2020, Bank of America estimated that fraud in California's unemployment benefits system alone could now total $2 billion in losses. Bank of America stated they identified 640,000 accounts with suspicious activity that should be investigated to determine whether they are bogus and should be shut down.
- The total number of members registered within underground channels devoted to unemployment fraud have been on the rise. One channel monitored by Recorded Future analysts had approximately 7,500 members at the beginning of November 2020. A month later, the total membership exceeded 18,000 members, with new messages uploaded by an administrator of the channel on a regular basis garnering several thousand views on average.

Reliance on Money Mules

Money mules likely remain a critical component of the unemployment fraud supply chain as evidenced by images uploaded by underground sellers of fraudulent unemployment methods and open source reports surrounding the arrests of suspected mules throughout 2020. The COVID-19 pandemic has forced reshipping mule operators to alter business strategies this year. A USSS advisory reported that the suspect fraud ring behind these filings already possessed a substantial PII database to submit the volume of applications observed earlier this year. Additionally, the USSS said the fraud network is believed to consist of hundreds of money mules.

Mules are essential for fraudsters who require a commodity to be physically moved from one place to another, or when fraudulent funds need to be moved between accounts. In money mule schemes, the scammers will also often recruit individuals to receive direct deposits from the fraudulent transactions, and then forward the bulk of the illicit funds to the perpetrators, keeping a percentage as payment for their efforts. The increased number of arrests around the country with a nexus to fraudulent unemployment relief claims has also provided clarity that multiple strings of fraudsters are likely operating independently with no direct nexus to any overseas operations.

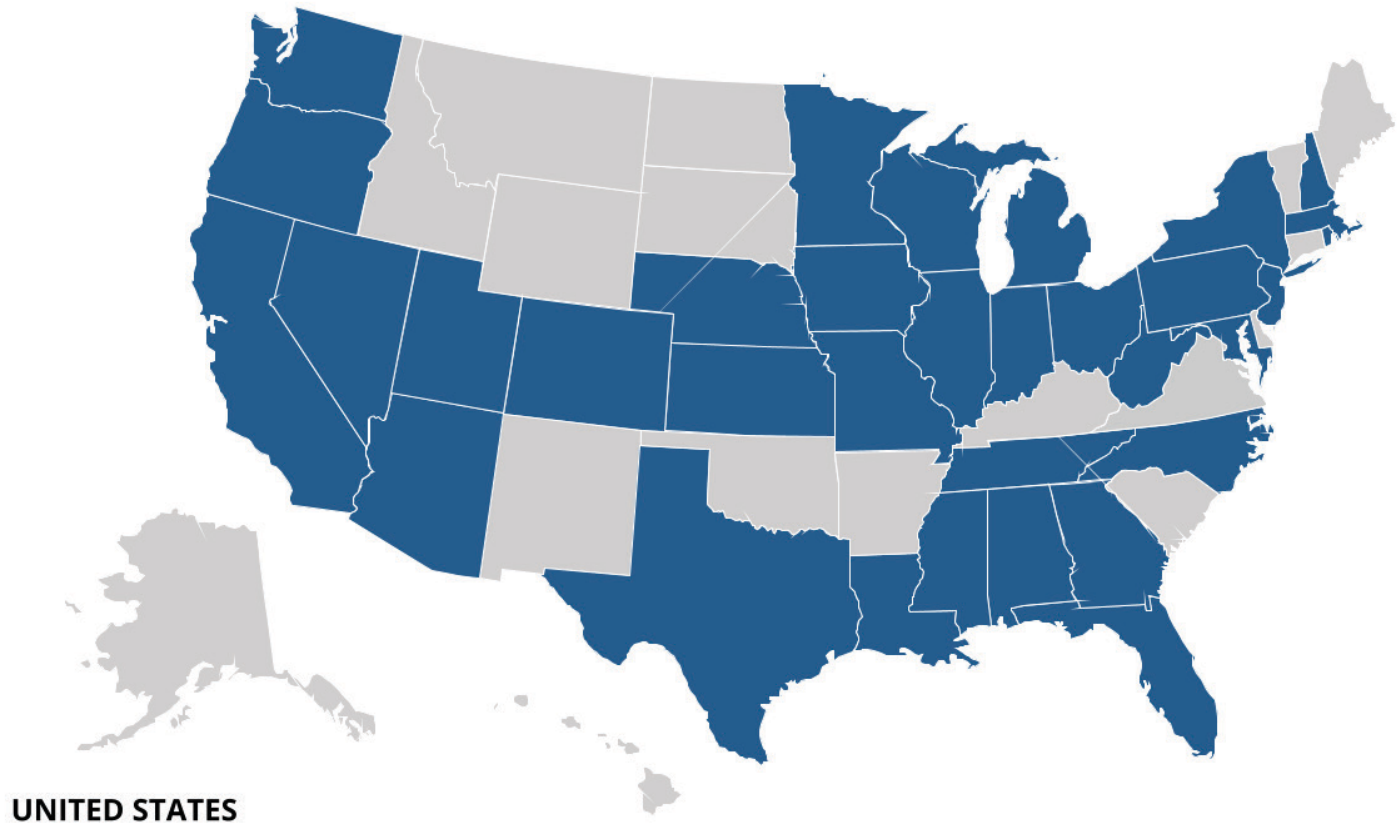

Figure 11: States referenced in unemployment fraud ads in the underground since November 2020 (Source: Recorded Future)

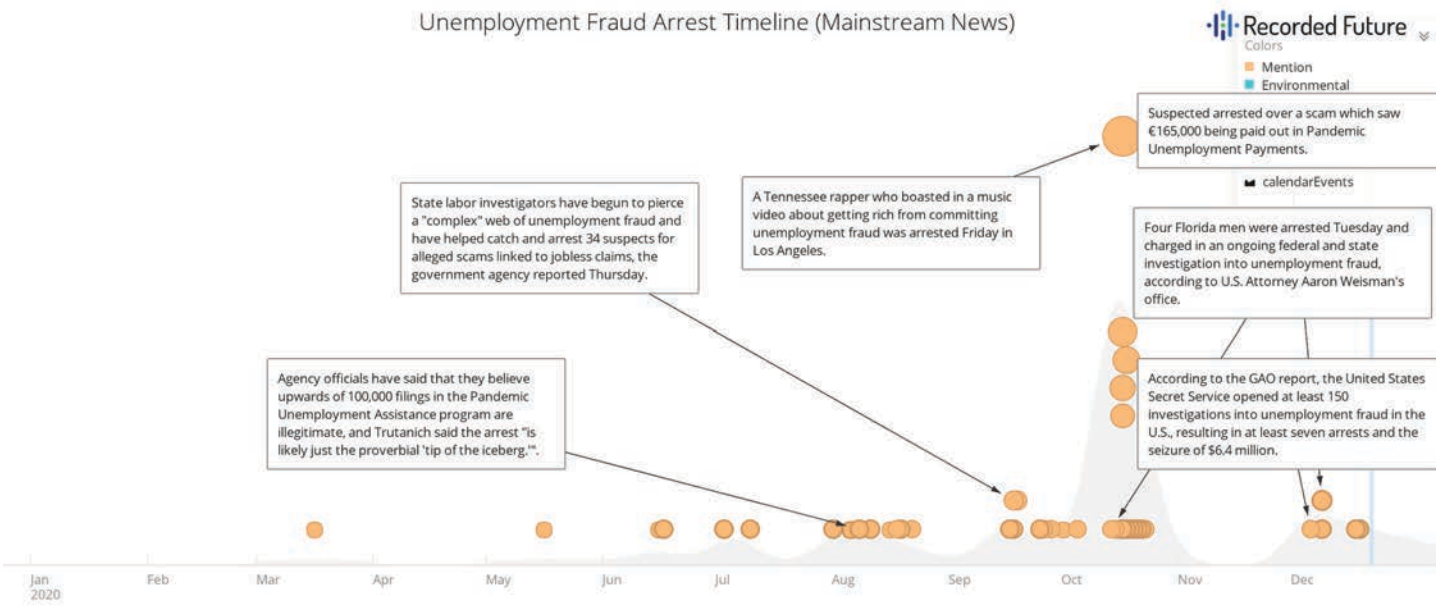

Figure 12: Unemployment fraud 2020 arrest timeline (mainstream news sources) (Source: Recorded Future)

- In September 2020, Attorney General (AG) Josh Shapiro of Pennsylvania (PA) announced charges against 20 inmates and accomplices, charged with committing unemployment fraud in three state prisons in central and eastern Pennsylvania. The AG's office stated there were also six individual inmates arrested without any known links to a ring.
- Posts from underground marketplace vendors observed as recently as October 2020 reveal that money mules likely play an integral part in assisting operations advertised on dark web sources.
    - On October 25, 2020, a member of the forum Omerta began advertising cash-out services for fraudulent unemployment claims in the U.S. The threat actor stated that their money mules ("bank drops") can cash-out unemployment funds for a separately negotiated percentage of the bank transfer.

Mitigations

A federal fraud investigator who spoke with KrebsOnSecurity in May 2020 on the condition of anonymity said many U.S. states do not have enough controls in place to detect patterns that might help better screen out fraudulent unemployment applications, such as looking for multiple applications involving the same IP addresses or bank accounts. The investigator went on to clarify that in some U.S. states, fraudsters need only to submit someone's name, SSN, and other basic information for their claims to be processed. The investigator is reported to have implied that the list of questions about a claimant's previous employer for authentication purposes, at some agencies, had diminished or been entirely eliminated as a result of the pandemic.

States have begun adopting their own individual measures to address the risk posed by this form of fraudulent activity. Representatives from states such as Massachusetts previously stated that they had begun implementing additional identity verification measures that will temporarily delay the payment time frame for many unemployment claims. As a result of these measures, certain unemployment claimants may be asked to provide additional identity information in order to verify the validity of their claim.

Organizations that suspect their employees have fallen prey to unemployment fraud scams can do the following:

- Relay the information regarding this fraud to the appropriate office at your local state level and USSS field office. The USSS has also encouraged victims to continue to liaison with local financial institutions to identify mules and potential seizures.
- Use features in monitoring software or applications that are capable of flagging potential spam or scams for payments in the app and sends text messages to users when it detects suspected fraud. Flagging potential criminal activity using tools and data sets to verify the identity of a claimant can help stop fraudulent activity before it begins.

Outlook

In a number of cases, the most important component for unemployment or insurance claim fraud is access to victim PII. This type of information can be accessed and purchased on a number of dark web marketplaces, shops, and forums for fairly low prices by anyone with enough knowledge to set up an account on underground sources. It is difficult for us to determine which of these fraud types are being carried out with the greatest frequency based on available data. However, scam activities that depend on PII will likely continue to spike following the release of some larger data dumps, especially any that are widely publicized and easily accessible.

About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.