



Threat Intelligence Memorandum

FEBRUARY 20, 2021

Executive Summary

ID.me will activate NIST 800-63-3 Identity Assurance Level 2 with an additional control, Face Liveness, in all states where we gate new UI and/or PUA claims unless there are operational blockers. ID.me will upgrade policies as soon as is feasible on a state by state basis.

On February 19th, ID.me identified an attack vector targeted at the device/telecom verification step. In late December, ID.me investigated 34 verified accounts that went through IAL2 with an additional Liveness check. ID.me's duplicate face checker successfully flagged the attacker's face as a duplicate and tied the duplicate face to multiple different identities and claims.

The attacker's ability to defeat the telecom verification step sparked a deeper investigation. Of note, all 34 accounts were tied to T-Mobile. We sent the accounts in question to T-Mobile and found the attacker was using a T-Mobile service to claim phone numbers that used to belong to different victims: (<https://www.t-mobile.com/support/account/change-your-phone-number>).

A recycled phone number targets a gray space in the ecosystem. Mobile Network Operators do not treat a phone number change in the same manner as a SIM Swap, moving an assigned phone number to a new SIM, or a Phone Port, moving a phone number to a different carrier. The old phone number typically also matches the victim's identity in financial records as well.

Problematically, phone numbers are often disconnected and reconnected when an individual doesn't pay their bills on time. After the balance is paid, the telecom will restore service and the phone number to the individual's device. As a result, this pattern is tied to individuals who have less money and therefore to many legitimate unemployment claimants. The attacker is able to blend into this pattern that is tied to many legitimate individuals who need money.

New claims are most vulnerable to this attack vector. For states screening high risk claimant pools, the attacker often does not know which identity is eligible to go through ID.me, and the identity might not have an old phone number available for claim as many old phone numbers are recycled and assigned to legitimate users. In those cases, the number is not available for the attacker. Because any identity can file a new claim, the attacker can target a bigger pool.

Controls to Block Fraud

- 1. Duplicate Face Detection:** On February 8th, ID.me operationalized Duplicate Face Detection. **This service represents a major technological breakthrough in fraud prevention.** Duplicate Face Detection examines a selfie – collected either through Unsupervised Remote or Supervised Remote (video chat) – to see if the same face is tied to additional accounts. This service flags duplicate faces in real time, and it has

proven remarkably accurate. All flags go through a human review to confirm findings prior to a report. In combination with Face Liveness, which ensures the selfie is the face of the user, Duplicate Face Detection is flagging the faces of the attackers who are able to get through telecom, document, and records checks. We have identified many criminals through this capability, and we are able to pass along the information to law enforcement while also suspended all identities and claims tied to the criminal's face.

2. **MSISDN Reporting:** The International Mobile Subscriber Identity (IMSI) is tied to the SIM and does not change. The Mobile Station International Subscriber Directory Number (MSISDN), the phone number, is used to route calls to the subscriber. A SIM might be associated with multiple MSISDNs or phone numbers over time. We are adding reporting capabilities with the telecoms to identify MSISDN changes. T-Mobile appears to account for about 80% of the attacks so we are honing in on T-Mobile first.
3. **SIGINT Ambushes:** We are implementing controls to re-direct high-risk traffic to video chat identity proofing to both deter attackers and to create a recorded video session law enforcement can use later to prosecute them. This re-direct will still enable legitimate claimants to verify their claim while also ensuring ID.me can block fraud. We need to tune these signals carefully to avoid snaring too many legitimate claimants in the filter.

Controls to Remediate Fraud

1. **Historical Phone Number Analysis:** ID.me is able to look back in time at the phone numbers used during identity verification to see if there were subsequent phone number changes associated with the device and SIM after the verification date. The attacker is using a single device and SIM to circulate through different phone numbers, so we are able to isolate on this pattern and to identify the associated IP addresses and claims.
2. **Fraudulent Claims Reporting:** We will circulate a list of claims tied to this pattern.

Summary

NIST 800-63-3 IAL2 with Face Liveness enables us to block this attack vector and synthetic fraud. We may be able to move back to an LOA3 policy at a future date once additional telecom reporting controls are in place. In the interim, Duplicate Face Detection ensures we are able to capture bad actors who attempt to target new claims flows. The telecom attacks appear to be driven by a relatively small group of actors who attempt to file a large number of claims. The concern now is that attackers might move to target our LOA3 or IAL2 flows which don't have the selfie with Liveness component. We can use data from the next week to assess.

ID.me



Very Respectfully,

Blake Hall

BLAKE HALL, CEO, ID.ME