Misuse of a Mobile Driver's License (mDL) Investigative Aid

Identifying Digital Evidence for the Suspected Misuse of a Mobile Driver's License (mDL) to Open a Financial Account

Science and Technology

02-2024

OVERVIEW

Mobile driver's licenses are gaining traction in the United States, though implementation varies across the nation. A mobile driver's license (mDL) is a digital representation of a state-issued driver's license that is stored on a mobile device. Cases of identity fraud associated with digital identities will likely increase **as mDL usage becomes more widespread.** As a result, investigators will need to be prepared for this new technology and know what type of evidence may support investigations. Recent cases highlight the need to understand how mDLs will impact future law enforcement investigations.

RECENT CASE: 2020 mDL Financial Fraud

The state of Louisiana experienced one of the first cases where a criminal used an mDL to fraudulently open financial accounts. The criminal obtained personally identifiable information (PII) from the victim to access the victim's mDL and generate additional fake documents (e.g., W-2, lease agreement). He then leveraged these items to open accounts with several financial institutions across the state. Thankfully, the criminal admitted guilt for the crime. Investigators also had access to key pieces of information, including but not limited to:

- Electronic time stamps that confirmed when the mDL was accessed
- Video surveillance showing the crime taking place at financial institutions

As a result, the investigation was straightforward. Many future cases, however, may not be so fortunate.

PURPOSE OF THIS DOCUMENT

This document gives investigators a foundational understanding of digital evidence that may be collected for a crime where someone leveraged an mDL to fraudulently open a financial account in person. This investigative aid also has an accompanying Investigative Aid Reference Guide that provides additional details on relevant evidence.

Layout

Stages: The investigative aid walks the reader through three stages that are relevant to obtaining and using an mDL: Opening Account at Department of Motor Vehicle (DMV), Provisioning with Digital Wallet, and Verifying Identity at Financial Institution.

Activities: The investigative aid walks the reader through the general activities that must occur for the crime.

Evidence: In alignment with the activities, the investigative aid provides an overview of potential digital evidence unique to leveraging an mDL, as opposed to a physical driver's license.* Information includes:

- **What:** What evidence can be used by law enforcement?
- **Why:** Why is this evidence important to build the case?
- **Who:** Who owns or has access to the evidence?
- **How:** How can law enforcement obtain the evidence?

Pain Points: The investigative aid highlights potential challenges obtaining digital evidence.

Assumptions

- The mDL issuers and verifiers will follow the standards, guidelines, and regulations identified below.
- The evidence identified in this document may be available for law enforcement to request. Note that pain points highlight some potential challenges in gathering specific types of evidence.

Standards, Guidelines, and Regulations

- ISO/IEC 18013-5:2021 Personal identification
  - ISO-compliant driving license
  - Part 5: Mobile driving license (mDL) application
- AAMVA Mobile Driver's License (mDL) Implementation Guidelines
- NIST SP 800-63-3 Digital Identity Guidelines.
- U.S. Customer Identification Program

**Note: Other relevant evidence that is not unique to an mDL but may support the chain of evidence is referenced in the Investigative Aid Reference Guide.*

STAGES	Opening Account at DMV	Provisioning with Digital Wallet	Verifying Identity at Financial Institution	
ACTIVITIES	**1.** Establish record with issuing authority	**2.** Add mDL to digital wallet	**3.** Present mDL to financial institution	**4.** Confirm mDL matches customer / **5.** Approve opening bank account
EVIDENCE	**WHAT:** Identity record including digital photo of suspect. **WHY:** Comparison between individual image stored at the Issuing Authority / State-Level DMV* to biometric (something the mDL holder is). **WHO:** State-Level DMV. **HOW:** Law enforcement (LE) officers and investigators use LE databases such as National Law Enforcement Telecommunication System (NLETS) to obtain digital photo.	**WHAT:** Date and time stamp of when the mDL app was downloaded. **WHY:** Build the context and timeline of criminal events. **WHO:** Digital wallets storing mDLs (e.g., Apple, Google, Samsung, third-party app store) and/or state-issued mDL app. **HOW:** Subpoenas directed to appropriate point of contact at the specific digital wallet storing mDL and/or state-issued mDL app. **WHAT:** mDL digital object, supporting data, logs of State-Level DMV's interaction with mDL device (outcome). **WHY:** Build the context and timeline of criminal events. **WHO:** State-Level DMV. **HOW:** Subpoenas directed to appropriate point of contact at the State-Level DMV. **WHAT:** Temporary image of suspect (license). **WHY:** Comparison between individual image stored at DMV to biometric (something the mDL holder is) temporary image of individual taken during mDL digital wallet registration process. **WHO:** Digital wallets storing mDLs and/or state issued mDL app. **HOW:** Subpoenas directed to appropriate point of contact at the specific digital wallet storing mDL and/or state-issued mDL app.	**WHAT:** Data that was shared and information about the identity of the mDL verifier. **WHY:** Build the context and timeline of criminal events. **WHO:** Digital wallets storing mDLs and/or state-issued mDL app. **HOW:** Investigator needs access to suspect's phone. **WHAT:** Logs of a State-Level DMV's interaction with an mDL device. **WHY:** Build the context of criminal events. **WHO:** State-Level DMV. **HOW:** Subpoenas directed to appropriate point of contact at the State-Level DMV.	**WHAT:** Record of mDL scan for verification. **WHY:** Build the context and timeline of criminal events. **WHO:** Cooperative suspect. **HOW:** Investigator needs access to criminal's phone. *May potentially be able to get this from financial institution if they are tracking the mDL scans. **WHAT:** Data that a financial institution is required as stated by the Customer Identification Program (CIP) data requirements. **WHY:** Build the context and timeline of criminal events. **WHO:** Financial institution. **HOW:** Subpoenas directed to appropriate point of contact at financial institution.
PAIN POINTS	Subpoenas may need to be directed to appropriate point of contact at the State-Level DMV. Some DMVs will not honor any out-of-state subpoena (e.g., New York) unless a judge from the same state has ordered that the DMV comply with the subpoena.	**Apple Wallet:** Provides Apple device or customer information if Apple has access to the information based on its data retention policies. Apple has temporary access to certain information (e.g., selfie, video of head and facial movements, subset of data from barcode on ID), but this information is deleted from Apple servers right after sending request to the state. **Google Wallet:** Shares personal information outside of Google if company has a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to meet any applicable law, regulation, legal process, or enforceable governmental request.	**Apple Wallet:** Presentment history is encrypted and stored only on the device, and Apple doesn't retain any presentment information that can be tied back to individual. **Logs:** Some states may not have access to logs of a State- Level DMV's interaction with an mDL device.	**Uncooperative Suspect:** Most mobile devices are encrypted with unrecoverable key by manufacturer. **FI:** May use third-party verification service, which could complicate evidence collection

Legend: Mobile Driver's License (mDL) Holder | Financial Institution

Science and Technology

Engage with Us

@dhsscitech

dhs.gov/scitech

Technologically Speaking Podcast

Science and Technology