Mitek

Verifying identity in a digital economy, where risk is on the rise

An ex-cybercriminal's take on fake-ID use and fraud

BRETT JOHNSON, EX-FRAUDSTER

A **NASDAQ**® company | **miteksystems.com**
San Diego | Amsterdam | Barcelona | London | New York | Paris | St. Petersburg

Mitek

The United States Secret Service called him “The Original Internet Godfather.”

Why? Thirty-nine felonies, a place on the United States Most Wanted List, one prison escape and the masterminding of the first cybercrime community, ShadowCrew, the precursor to today’s darknet markets. Brett Johnson laid the foundation for the way modern cybercrime groups operate to this day; identity theft, forgery, computer crime, tax return identity theft, credit card fraud, account takeover, money laundering, fake ids, phishing are the most common crimes.

After serving seven and a half years in federal prison, Johnson pivoted on his path in life. Now, he’s a dedicated security consultant specializing in cybercrime and identity theft. His years as a cybercriminal gives him an intimate understanding of cybercrimes and fraud, not often accessible to the average business or financial institution.

We’ve recently partnered with Johnson for his insider’s take on fraud. In this report, he defines the different types of cybercrime and how fraudulent identity documents are used to commit these crimes, what security methods are no longer affective in mitigating risk, and what the future may look like for the role of digital identity verification in fraud reduction. Here is his take:

Straight from the fraudster’s mouth

In addition to its actual criminal activity, ShadowCrew was also a teaching environment. If someone approached us looking to commit a type of crime and didn’t know how, we would teach them. We posted tutorials and held classes. We offered individual instruction.

I ran ShadowCrew — and I was also one of its teachers. I taught criminals how to phish, commit tax-return fraud, institute account takeovers, launder money, defraud people, and much more. I taught members best practices on using fake IDs.

Many of the crimes involving the use of fake IDs remain the same today, however two things have changed since then:

- **The quality of fake IDs has improved dramatically.** Today, fake IDs are available in all 50 states and in every country. Holograms are real. UV ink and microprint are present. Any OVD (Optical Variable Device) on a real driver’s license is now present on a fake one. Where it was once possible for the untrained, naked eye to determine if a license was forged, it is now nearly impossible.
- **A criminal has easy access to anyone’s personal information: name, social security number, DOB and more.** Fraudsters can now create or purchase near perfect fraudulent ID cards with correct information on them, presenting a significant problem for companies attempting to verify the identity of a user.

Cybercriminals are upping their game. Their techniques are becoming more sophisticated, forcing businesses and ID verification providers to leave ineffective methods behind, look to the future, and ensure their technology remains several steps ahead.

Mitek

Yesterday's identification techniques are a dying breed

The demise of KBA

Knowledge Based Authentication: KBA … those security questions that are asked when s omeone applies for credit, opens bank accounts, transfers funds, requests records, credit reports and more. Answering these questions correctly authenticates someone's identity. And once the person answering the KBA questions is authenticated, he/she can do whatever they choose.

Identity thieves love KBA. All a thief needs to do is answer those same security questions and they can access your credit report, your IRS tax transcripts, your bank account and much more.

"LAST YEAR ALONE SAW 1500 REPORTED BREACHES. OF THOSE 1500 BREACHES, MORE THAN 2.6 BILLION RECORDS WERE COMPROMISED..

…that's right, more than two billion records in one year. These types of breaches have been going on for decades and will continue for decades."

After that, they can open new accounts, drain existing accounts, divert government benefit payments, apply for loans — anything. The only thing a thief really requires are the answers to those knowledge-based authentication questions.

Obtaining those answers isn't always a difficult task.

The amount of personal information available and accessible to identity thieves is staggering

Criminal website Robocheck.cm advertises the social security numbers and dates of birth for more than 170 million Americans at $2.90 each. Jstash.Bazar — running on the Blockchain DNS and touting Equifax breach data — claims to have even better SSN and DOB lookups at the same price. Complete identity profiles sell on criminal websites for $30 to $130 depending on the location of the victim, the gender and the credit score. Did you know that children are the number one victims of identity theft? That's right. One in four children will be a victim. For $2, a criminal can buy a child's PII: Information that includes the child's name, date of birth, social security number, mother's maiden name and place of birth. Credit card information routinely sells for under $20. Bank account, PayPal or other payment processor logins sell in the $40 range. Customer logins for major retailers sell for $3.00. Credential dumps — mass amounts of logins with password — are often posted free on Pastebin or as a torrent.

CRIMINALS ALSO RELY ON LEGAL SERVICES TO OBTAIN PII

Services like BeenVerified, Spokeo, Intellius, WhitepagesPro and Pipl are often utilized by criminals to obtain information. BeenVerified offers unlimited background checks for under $20 per month. Services like Delvepoint and TLOxp — which deliver an in-depth background and identity lookup usually available only to government agencies, skiptracers and collection bureaus — are sold for $80 each on criminal marketplaces.

NOW ADD IN THE AMOUNT OF INFORMATION PEOPLE SHARE ON SOCIAL MEDIA SITES

LinkedIn often gives a complete work history which a thief can access. Facebook yields birthdates, mother's maiden names, relatives, friends, previous addresses and more.

If someone thinks they can do something to stop a criminal from accessing their information, they are wrong. As such, KBA, knowledge-based authentication, is dead.

Financial institutions, government agencies and credit bureaus are keen to fraudster know-how and have been implementing two-factor authentication as an additional means to confirm identity.

Mitek

Two-factor authentication as it is commonly used is also becoming more ineffective

Two-factor authentication is often implemented via email or mobile device. A person tries to log on to a website and a code is sent to that person's email account or as an SMS message to a cellphone. The person then confirms receipt of the message and gains access.

TWO-FACTOR IDENTIFICATION VIA EMAIL IS USELESS

Email accounts are routinely compromised because of weak passwords, failure to update passwords after a breach, and use of the same passwords across multiple websites. Passwords of specific individuals are commonly acquired via spearphishing, which is estimated to be over 80% successful.

SMS FOR TWO-FACTOR AUTHENTICATION DOESN'T FARE ANY BETTER THAN IT DOES FOR EMAIL

The proliferation of SIM swap attacks and the recent SS7 exploits prompted the National Institute for Standards and Technology (NIST), to issue a warning against using SMS to authenticate identity.

Given the problems of KBA and two-factor authentication, verifying an identity online is problematic. Many financial institutions and online merchants request pictures of driver licenses, selfies holding the license, live video feeds of driver licenses, and more to authenticate identity.

With KBA and two-factor identification methods on the outs, the fake ID business is booming

THE USE OF FRAUDULENT IDS AMONG ORGANIZED CYBERCRIMINALS

In the early days of cybercrime, fraudulent IDs were difficult to acquire. ID makers were few and the selection of US states limited. ID makers spent dozens of hours creating the driver license template manually using a copy of a real driver's license and Photoshop. IDs were often printed on Teslin instead of PVC to save costs. Real holograms weren't available, so gold interference was used to mimic the hologram. Quality was hit or miss. Fake IDs were never good enough to allow a criminal to use a fake ID in the same state it was issued. Further, the limited variety of states available meant that criminals had trouble replicating a victim's actual driver license. Victims were targeted from states where fake IDs were available. This allowed a crook to use an accurate driver license with correct details and a different picture on the ID.

TIMES HAVE CHANGED.

Today, the quality of fake IDs is good enough that a criminal can use a driver's license in state. Real holograms are present. UV ink, raised printing, and other security features are present. All 50 US states are available. Every country is available. Federal authorities have shut down most of the US based suppliers, so fake IDs are typically shipped out of Hong Kong. They sell for under $80. Some criminals need scans or photos of a fake driver license with someone else's picture on it. Numerous services like Secondeyesolutions.ch provide such for $30. If an institution requires a selfie with the ID, Secondeye sells those for $50.

The quality of the fraudulent products is outstanding. To the naked eye, they look real.

WITH FAKE ID IN HAND, THE ONLY QUESTION IS:

What type of crime will be committed?

Mitek

Types of crime requiring the use of fraudulent IDs

There are a variety of crimes which require a criminal to use a fraudulent ID at some point.

- **Synthetic fraud:**
  Combining real and fabricated information to create a new credit profile. Once created, the criminal then opens fraudulent accounts and makes purchases on those accounts.
- **New account-opening fraud:**
  Using stolen or fraudulent details to open an account with the intent to commit fraud.
- **Account takeover (ATO):**
  Using stolen or counterfeited credentials to assume control of (usually) an online account. The primary purpose is to assist in monetary or credit card theft.

Synthetic fraud

In 2011, the Social Security Administration randomized all new social security numbers (SSNs). Doing so meant it was no longer possible to determine the year the social was issued nor the state it was issued in. The move was supposed to combat identity theft. For individuals issued an SSN prior to 2011, if a thief knew the last 4 digits of someone's SSN, it was easy to get the first five numbers. The SSA plan worked. That specific type of identity fraud was stopped.

But the move created a larger problem: Criminals could now fabricate social security numbers. Following the SSN algorithm, a crook could create a nine-digit number. If, after running the number through a social security number validator the number came back as unissued, the thief could use it as an SSN to commit synthetic fraud.

A criminal could also use an ITIN, or an SSN belonging to someone incarcerated for a long period.

The most popular way to commit synthetic fraud is to use a child's SSN issued after 2011. Using a kid's SSN, a fraudster adds a name to it, an adult date of birth, an address, and a phone number.

The fraudster then applies for credit. The way the credit bureau system works is: If an application is submitted, and the bureau has never seen the data before, the application will be denied. But, when it is denied, it builds a credit report in the system with that information. The synthetic profile now has a credit report. The credit report is a new, zero-credit history, very thin file. The idea now is to pump up the credit score as fast as possible and cash out.

FIRST STEP: OPEN SOURCE INTELLIGENCE (OSINT)

When applying for credit, many systems look for information outside of what is on the credit report. A search is undertaken for public data related to the applicant. Listyourself.net is a free Whitepages listing service. The fraudster inputs the synthetic information into it. Two weeks later, an address and phone number is associated with the synthetic identity. The fraudster may also opt to open a Facebook, or other social media accounts in the name of the synthetic identity.

The fraudster can now open rewards accounts at grocery stores, airlines and pharmacies.

Mitek

OSINT IS TAKEN CARE OF. NOW IT'S TIME TO BUILD CREDIT.

Most fraudsters go to CapitalOne and apply for a secured card. CapOne gives a $200 credit line for a $39 deposit. The fraudster is already profiting on the synthetic profile. The secured card doesn't do much for the credit score, but it does give the synthetic identity a primary line of credit.

To boost the credit score, the fraudster usually relies on credit piggybacking through authorized user trade lines. It's a legal practice in the US used by many to boost credit scores. Adding an authorized user to a credit card automatically makes that card's specific history become the authorized user's history after the next reporting cycle. If the card used has good credit, good debt ratio, and has been open long enough, a synthetic profile can go from a poor credit score to a high 700 score in 30 days.

Authorized user trade lines have an additional benefit. It ages a new credit profile. A card with 10 years of history added to a week-old credit profile will cause that profile to appear 10 years old.

Once the synthetic profile reaches the desired credit score, the fraudster can profit.

However, opening new accounts requires documents. Applications for credit, loans or starting bank accounts in the synthetic profile's name often require a copy of an ID. If a fraudster cannot acquire the needed ID, or if the ID doesn't pass verification, he will be unable to profit from the crime.

Identity documents used to commit synthetic fraud:

- **A physical driver's license with his picture but the synthetic identity's information on it.** This is presented at physical locations to open new accounts.
- **Online driver's license photo, scan and selfie with someone else's picture and the synthetic identity's information on the document.**

New account-opening fraud

Whether committing synthetic fraud or simply engaging in traditional identity theft, opening new accounts is one of the main reasons for a criminal to use a fraudulent ID.

Fake driver's license use in synthetic fraud differs from traditional identity theft in that the documents created for synthetic fraud contains a majority of fabricated information. Driver's licenses created for traditional identity theft tend to have the correct DL information of the victim, but with a different photo.

It's important to note that when committing synthetic fraud, KBA isn't an issue as the fraudster creates the profile of the synthetic identity and therefore knows the answers of any security questions which might be asked.

Opening accounts when committing traditional identity theft involves acquiring a complete identity profile to defeat KBA and obtaining fake IDs to satisfy any requests for documents.

Depending how the new account will be opened determines whether the fraudster needs a physical driver's license or a virtual one. Committing new account-opening fraud often involves walking into a business to open the account. This is common with bank accounts and various merchants at certain times of the year. For this crime to be successful, the fraudster needs an ID with the victim's information on it. The fraudster also needs to memorize basic KBA information to answer any questions which might arise. Opening new accounts in person tends to be easy. The clerk or teller looks at the ID just long enough to see that the data matches. They look for a hologram and feel raised printing. They place the ID under a UV light to see if ultraviolet ink is present. It's a cursory examination lasting a few seconds; real scrutiny of the ID never takes place. The fraudster has only to defeat the person he hands the ID to.

Submitting documents online is more complicated on one hand, but also easier on another, for the fraudster. Answers to the KBA questions don't have to be memorized. The identity profile is in front of the fraudster for him to reference as needed. The fraudster doesn't need a physical ID. He doesn't need to show his face. He can put someone else's picture on the ID. If a selfie is required for the account, fake ID service providers provide individuals to take those selfies.

The worry for a fraudster comes in determining if the documents he is sending in are verified by more than a human eye.

Mitek

Account takeover (ATO)

ATO affects all manner of accounts: Email, merchant, bank, credit card, financial services, credit report, tax documents, social security profiles, entertainment services and more.

Taking over what cybercriminals consider low-level accounts (merchant logins, email accounts, streaming services,) rarely involves more than using stolen credentials and signing into the account. Depending on the website, the crook may act immediately or might wait in an attempt for the takeover to be considered legitimate after a certain amount of time passes.

For higher level accounts (financial services, government benefits), a thief needs the complete identity profile, called a "Fullz," among cybercriminals.

Fullz: The victim's name, address, phone number, SSN, DOB, MMN, DL#, background check, credit report and any social media information which might be interesting.

Once the identity profile of the victim is purchased or built, an identity thief can use the information to defeat a knowledge-based authentication system. Higher level targets often require identity documents.

The thief is usually unable to obtain the real driver's license of the victim or a snapshot of the real ID. As such, a fraudulent ID must be used. The fraudster can create his own template for the ID, but usually opts to buy one from a criminal marketplace or use a variety of fake ID services which cater to identity thieves. The ID will have the correct DL information of the victim on it, while the picture is of the fraudster if it's a physical ID or of someone else if it's a virtual ID.

Here are the types of identity documents criminals can use to commit ATO:

- **Physical driver's license with the victim's information on it, but the face of the fraudster.** A fraudster will use this type of document when a physical appearance is necessary; to pick up items, on certain applications for credit, or to withdraw money, for example.
- **Online driver's license photo, scan and selfie having someone else's picture on the document with the synthetic identity's information on it.**

Identity thieves rely on poor security, manual-only inspection of the documents by untrained humans, and the hope of simply getting lost in the traffic of legitimate customers for their fake ID to pass.

Mitek

Mitigating fraud with identity verification

SKILLED CRIMINALS USE FAKE IDS

The beginner crook doesn't have the confidence to hand someone a fake driver's license. She doesn't understand security well enough to trust sending one in online. She thinks she'll be caught, found out, and sent to prison. New fraudsters don't trust the quality of the documents and don't understand the security inadequacies of the institution they're trying to defraud. They also don't possess the skill. A newcomer in cybercrime is still learning how to remain anonymous and commit crimes, such as CNP fraud, which don't involve presenting documents. Presenting a fraudulent document in person or online means learning a new skill in addition to the others. A newcomer to cybercrime doesn't have the time to do all those things.

So, the use of fraudulent IDs — either in person or sent electronically — is typically a crime committed by more experienced, skilled criminals. The fraudster presenting a fake ID either in person or online has generally developed the skill to stay anonymous as well as the skill to commit a variety of different crimes. She realizes that 99% of the people visiting her target are legitimate customers. She knows that the institution doesn't expect a fraudster. She knows the institution will likely just look at the ID and not question it. She has committed enough crimes that she understands security seems as an afterthought at many institutions.

WHEN AND HOW DO CRIMINALS USE A FRAUDULENT DRIVER LICENSE?

Most fraudsters are reluctant to put their face on an ID. But that also depends on the circumstance. Walking into a retailer with a fake ID is much different from walking into a bank or check-cashing business with a fake ID. The security of a merchant or retailer is much lower than that of a financial institution. The chances of a financial institution capturing good video of the fraudster is higher than that of a retailer. Bank's employees tend to be better trained than retail employees. ID verification in retail tends to be a quick look at the driver's license and nothing more.

That isn't to suggest a fraudster won't walk into a bank with a fake ID. He will. But he will attempt to avoid it. He will try to find an online service which doesn't require a walk-in. He will try to get a "cashier" or "money mule" to walk in for him. But for the most part, even experienced fraudsters prefer to submit documents online without the risk of making a physical appearance or using their real faces on the ID.

But the problem for fraudsters with submitting documents online is that they don't always know what verification procedures the target is using to authenticate the driver's license.

For that reason, a fraudster will do as much research as possible to attempt to learn the security procedures of the target. He will read the Terms of Service hoping information is there. He may call in to socially engineer a customer service rep into divulging information. He may set up an account in his own name to study the process. He may conduct test runs to find how security works.

A fraudster does worry, though, when a fake driver's license is verified by a procedure other than a person. Fake IDs are good enough to fool the human eye — especially the eye of a poorly trained teller, cashier or customer service agent. Fake IDs are not good enough to fool the eye of machine learning and advanced algorithms. The counterfeit template, the handmade fonts, the photoshopped picture and more are recognized by the machine and flagged as fraudulent. The machine finds things a human won't. The differences between today's fraudulent driver's licenses and real driver licenses are so small, so subtle, that the untrained human eye is incapable of recognizing the differences. However, a combination of AI-powered machine learning, facial comparison biometrics and an expert manual review, when needed as an escalated layer, is comprehensive enough to catch more frauds.

Because after all, a fraudster will try and find a way to make money off of any institution with a profitable product or service. But fraudsters do understand that not all security is created equal. They search out rules-based systems and targets that don't employ proper security. They search out businesses with poorly trained employees who don't effectively spot fakes and poor or non-existent identity verification procedures. They search for less secure targets.

Mitek

PROPER SECURITY, DIGITAL IDENTITY VERIFICATION AND EXPERT MANUAL REVIEW DETER CRIMINALS AND REDUCE FRAUD

Proper security and training are necessities. Many in-house employees simply aren't equipped to catch sophisticated false identities and stop fraud in its tracks, leaving the business vulnerable to über-technically savvy criminals who will defeat the untrained, naked human eye. When a business can recognize these limitations, and the benefits of assigning computers with the task of identity verification, they can take steps into the future and stay ahead of nefarious cybercriminals.

Advanced algorithms and artificial intelligence accomplish what a person cannot. Fully automated machine learning techniques applied to document capture, biometric facial comparison, liveness detection, document authentication and classification and data extraction deliver near instant identity verification with outstanding results — with minimum friction for customers and the company. *It works.* In fact, the technology is so effective that fraudsters have started gravitating towards targets where they know only humans are examining documents, or where they know the verification company at hand isn't effective enough to recognize the quality of fake identity document in their possession.

Acquire customers. Mitigate fraud.

www.miteksystems.com/idv