IDENT SOLUTIONS

MLB | FEDCHECK

The MLB with the Power of Fedcheck
Scan. Protect. Peace of mind.

CONTENTS

ABOUT FEDCHECK

Fedcheck

You wouldn't buy a car without a Carfax. You wouldn't hire a new employee without their resume. So why would you let someone into your organization without understanding their threat level to your employees, patrons, IP, and your reputation?

Although you may use other security tools such as metal detectors, bag checks, bollards, and security cameras, FedCheck goes beyond these by giving you a complete digital criminal footprint. It is essential to every organization's security protocol. FedCheck is the new way to gain actionable intelligence and comprehensive situational awareness.

PURPOSE

The purpose of FedCheck is to help organizations identify risk to keep their facilities safe. With the scan of a Driver's License, FedCheck instantly runs a criminal history check – very similar to a background check.

FedCheck not only identifies individuals with a criminal past but helps mitigate risk by identifying individuals with a pattern of criminal activity, giving your security team, actionable data to help them do what they do best: protect.

UTILIZATION

FedCheck can be used to scan contractors, temporary workers, volunteers, and those accessing critical areas prior to entry. Simply scan individuals as they arrive and get an instant, comprehensive criminal check.

WHAT FEDCHECK SEARCHES

For ease of use, we've created 6 record types that can be turned on / off to customize your data to only the records you care about. Two of those categories have subcategories that allow you to truly personalize your FedCheck results.

1. WANTED PERSON

2. CRIMINAL HISTORY

3. ARREST RECORD

    a. Delinquency / Mischief

    b. Vehicle / Traffic

    c. Endangerment / Neglect

    d. Drugs

    e. Theft / Burglary

    f. Violence

    g. Unknown / Blank

4. SEX OFFENDER

5. TERRORISM WATCHLIST

6. SANCTIONED/BANNED LIST

    a. Athletic Sanctions

    b. Professional Organization

    c. Gaming / Casino Ban

    d. Healthcare Sanctions

    e. Government Sanctions

    f. Financial Sanctions

*Note: FedCheck DOES NOT check immigration status, nor identify demographic information such as sex and race.

GOVERNANCE

The data accessed through FedCheck belongs to you. The intent of this system is not to identify people with criminal history to prevent them from working. Rather the intent of the solution is to gain further awareness and improve the overall security posture through the identification of selected criminal patterns that pose a risk.801

SAFETY ACT DESIGNATED TECHNOLOGY

FedCheck has been recognized by the DHS as an innovative, effective anti-terrorism tool—and a powerful resource for those who protect our critical infrastructures and communities. Given SAFETY Act designation status, FedCheck is your best insurance policy.

BEST PRACTICES & POLICY

Admin & Users

FEDCHECK ADMINS
Your FedCheck Admin controls the program for your facility. They are the main source of contact whenever your FedCheck brings back a hit on a visitor and they are able to review the analytics on the FedCheck Dashboard. Note: There are no more than 5 admins allowed per FedCheck account.

USERS
Users are those within your facility that will be utilizing FedCheck solely for scanning and admittance purposes. These could be employees, event staff, etc.

Taking Notes

Make notes within FedCheck on each individual visitor. If a visitor has a Red Siren, make a note on the actions you took. If they were placed on Hold, make a note as to why. These can be used as records for future visits.

Placing on Hold

Treat this as your "waiting area" in FedCheck. Place any visitor on Hold in FedCheck while you wait for your Admin's next steps on whether or not to admit an individual. Your Admin can access the Holds and take the necessary next steps.

Facilities

Facilities are where you plan to use FedCheck. For example, if you are going to use FedCheck in your front lobby, you would title it "Front Lobby." Please check with your FedCheck Admin which facility to use or if you need to add another one.

Hits and Sirens

RED SIREN
Red sirens appear when FedCheck finds a "hit" or criminal record associated with an individual's name and DOB that it pulled from the scanned ID. If your FedCheck finds a hit, act calm and wait until your Admin provides next steps. Most facilities escort or keep an eye on those with a Red Siren, some even turn visitors away. How you deal with Red Siren's is completely up to you and what works for your security protocols.

You are also able to Red Flag a visitor. If a visitor has been Red Flagged, they should no longer be allowed access to the facility or business.

GREEN SIREN
Green sirens are new visitors whose ID didn't have a hit or returning visitors your security team has marked safe to admit.

ID Requirements

State Identification Card, Driver License, Passport, Visa, or other MRTD (Machine Readable Travel Document) are required to successfully run a FedCheck. If your organization does not already require identification to visit, you will need to update your security policy to do so before a FedCheck can run and admittance be granted. Check with your Admin to see if a grace period is established at your facility.

All visitors 18+ must have their physical ID scanned in FedCheck for admittance. Visitors under the age of 18 are exempt unless your security policy says otherwise. If your facility has many minor visitors/students, you may consider enforcing the following policy in addition to the ID recommendation.

ID WON'T SCAN

If you don't see any visible damage and nothing happens when you attempt to scan, it could be a fake ID, and we suggest no admittance. If you try to scan and get an error return stating "ID not recognized" or "Unable to process JSON" capture picture of both the front and back of the ID. You can then select the 'Can't Scan' button that is on the scanning screen of FedCheck and manually enter the guest's name, DOB, an ID number.

ID IS DAMAGED

If you can see visible damage and the ID will not scan, make a judgment on whether to allow them access this time but tell the visitor they need one that will scan next time. You can also use the 'Can't Scan' option to manually enter their name and DOB.

ID IS EXPIRED

Run FedCheck and allow or deny upon FedCheck return – give them one grace period to get a new ID that is valid.

TECHNICAL DIFFICULTIES

If technical issues are client side (i.e. device dies, app out of date, network/connection issues, etc.) refer to your FedCheck Admin for decisions on allowing or denying access.

If the technical issue is not client side submit support ticket to support@ident.solutions or access the chatbox on the Ident.solutions homepage. You can also use our VIP text option by texting (385) 315-9681.

Military ID

Ask for another preferred form of ID to run FedCheck– if they do not have another form of ID verify that the Military ID is not expired and is not a Dependent Military ID before allowing access. You can also manually enter their name and DOB using the 'Can't Scan' button.

Issues with Visitors

Visitor has no ID, refuses to provide ID, refuses to sign waivers, or any other issues with visitors that need escalation, do not allow admittance and refer to your FedCheck Admin.

FINDINGS REPORT

ACTIONABLE INTEL

FedCheck scanned a total of 175 visitors during the 2020 MLB NLCS Playoffs & World Series. Out of the total number of scanned visitors, 21% returned with a hit on their criminal record.
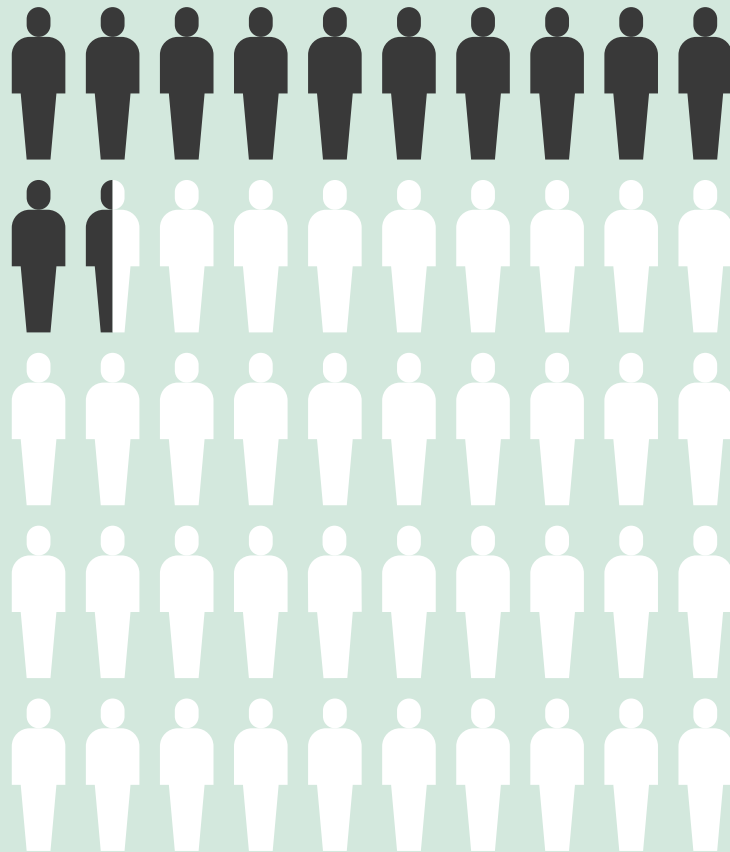
21% returned with a hit on their criminal record.

# Here's the breakdown. The most frequent criminal data we found:

Mischief: 11 %

Violence: 14.3 %

Endangerment: 28.7 %

Theft: 33.3 %

Drugs: 12.2 %
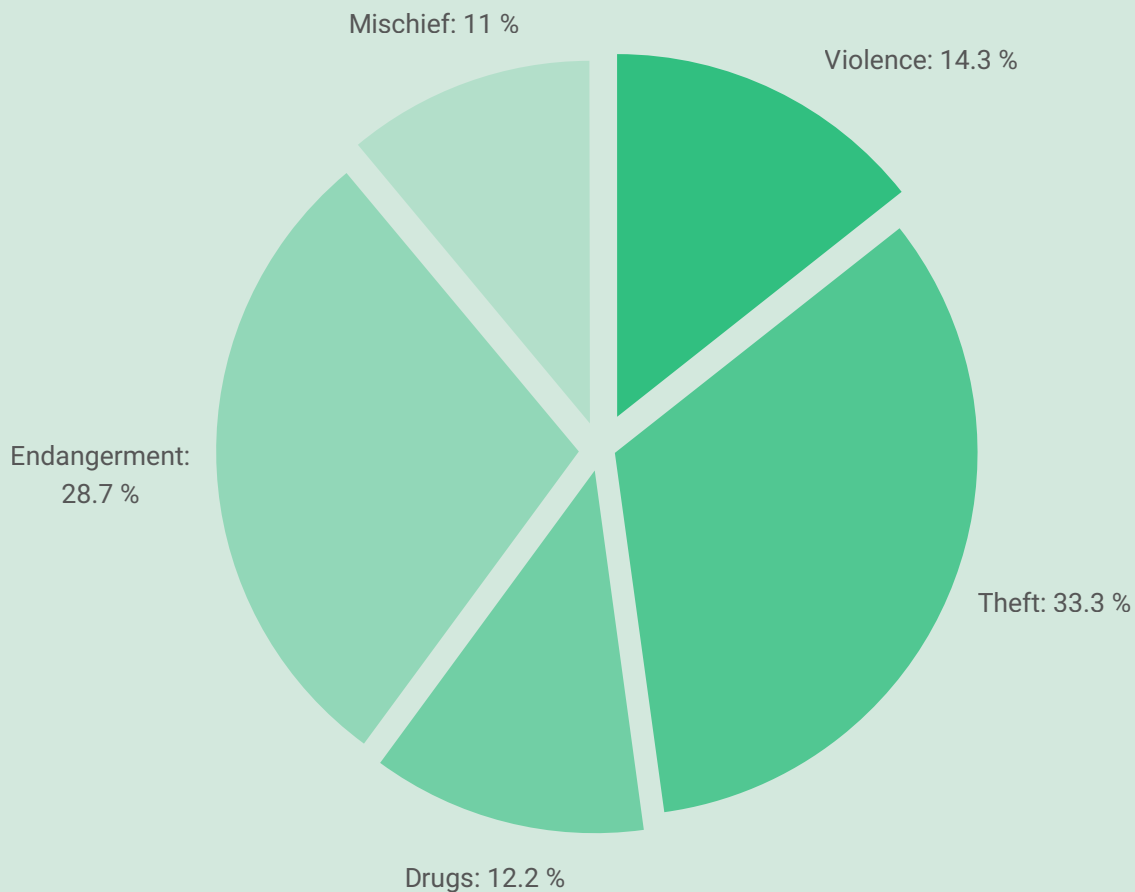
We recommend narrowing down to focus on the most egregious crimes including violence 14.3% and theft 33.3%.

Violent: 19.4% returned with recurring patterns of violent behavior
Theft: 44.4% returned with recurring patterns of theft

27.7%
VIOLENT RECORD

19.4%
RECURRING COUNTS

50%
THEFT RECORD

44.4%
RECURRING COUNTS
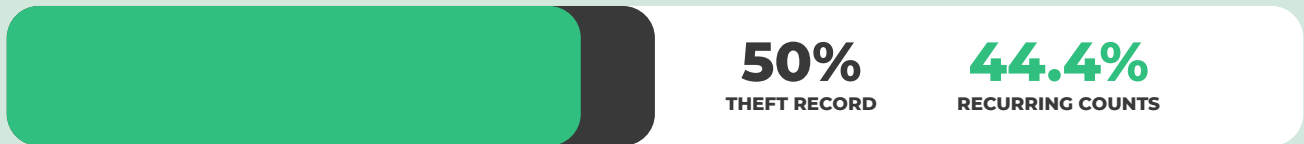
Out of the total 175 scanned visits, 5.7% came back with repeated violent offenses and 10.3% came back with repeated theft charges.

Picture this. Out of 1,000 people you allow:

57
would be a
violent threat

&

100+
would have a
threat of theft.

That being said, here's who was actually allowed inside your event:

One visitor's data returned with over a 10-year history of major Theft on their record and another visitor had a theft charge that ranged in value of $20,000 - $100,000.

One visitor had active warrants in the state of Texas.

A visitor's record returned with over 25-years of Theft, Drugs, and Violence.

A visitor was allowed inside the event with a 10-year history of Violence, including Assault and Terroristic Threats. Some of their charges were even as recent as 2020!

One visitor with a history of major theft showed up on 2 separate days during the event.

10 YEARS OF THEFT

ACTIVE WARRANTS

25 YEARS OF THEFT, DRUGS, AND VIOLENCE

TERRORISTIC THREATS

MAJOR THEFT

FINDINGS REPORT

DATAOLOGY

FedCheck's verifiable data resulted in an 84.8% accurate match rate. This found 70.4% with a full name and DOB, 7.8% including a mug-shot, and 6.6% with matching middle initials.

84.8%
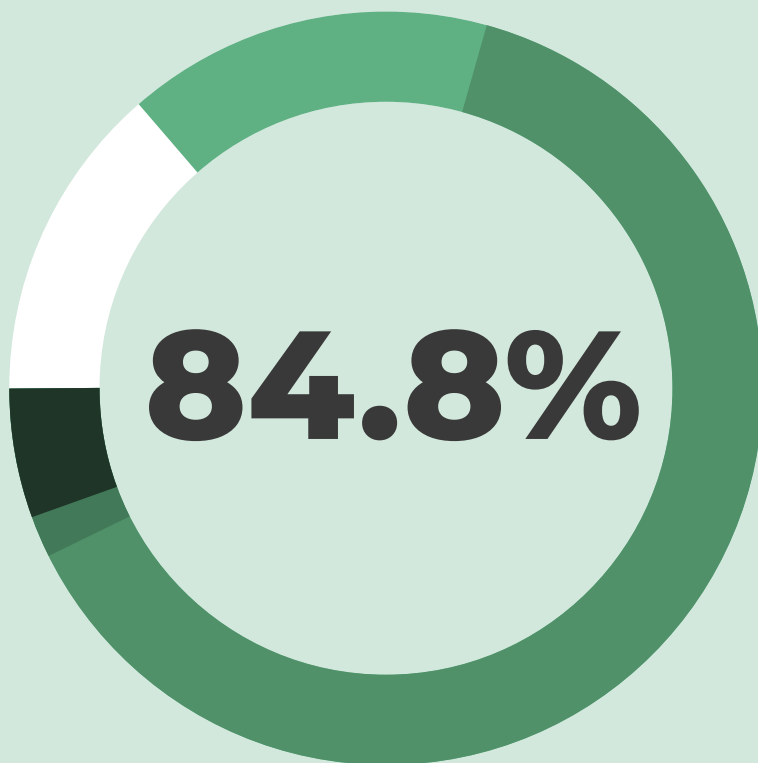
84.8%
Accurate Match Rate

7.8%
Full name match
with mugshot

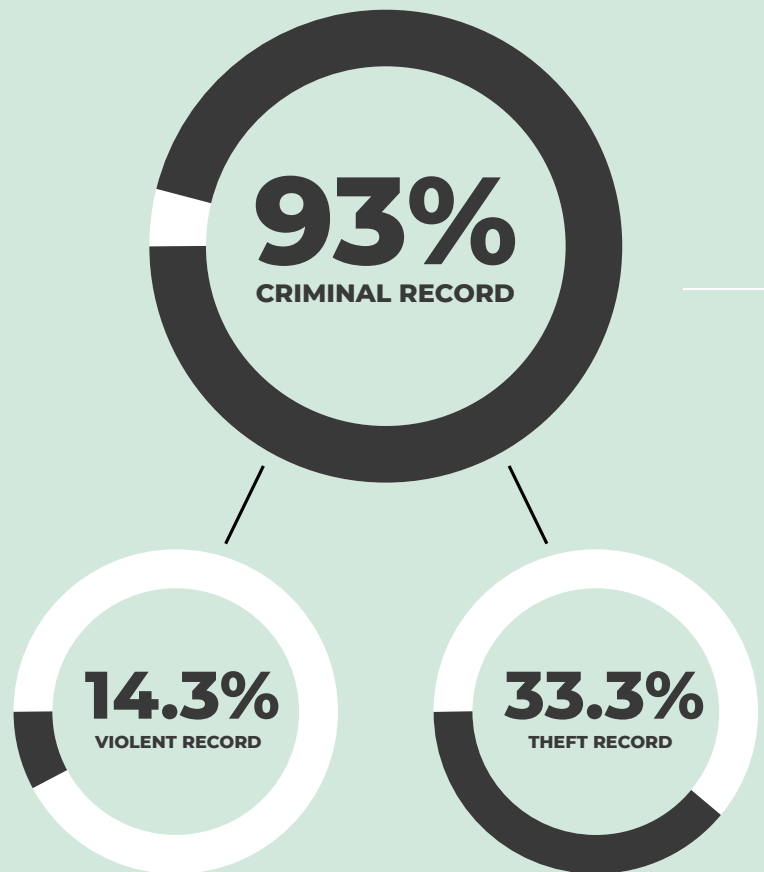**6.6%**
First name, Last name,
Middle initial, and DOB

15.2%
First name, Last name,
and DOB

Day	Visit Count	Visit %
10/13/20	**43**	**23%**
10/15/20	6	3%
10/16/20	2	1%
10/21/20	6	3%
10/23/20	**127**	**69%**

FedCheck found records from 8 states, 93% of criminal records coming from Texas alone.

TX	226	93.0%
CA	3	1.2%
OK	3	1.2%
FL	2	0.8%
AZ	1	0.4%
IA	4	1.6%
IN	2	0.8%
MD	2	0.8%

93%
CRIMINAL RECORD

14.3%
VIOLENT RECORD

33.3%
THEFT RECORD

FedCheck discovered the most hits from these police offense codes.

Other common offenses FedCheck found:

DUI / DWI	Theft / Burglary	Poss. Controlled Substance	Assault
20.2%	**26.7%**	**18.9%**	**13.2%**

FAQs

Why do we need to screen our visitors?

FedCheck helps identify risk to help keep your organization safe.

No reputable company would hire someone without doing a background check because the risk is too high, yet they will let thousands of visitors into their facilities without knowing anything about them.

The challenge is that although the visitor has gone through the check-in process, we still know nothing about them, they essentially have no identity other than a face and a name. With the power of FedCheck you are able to run an instant background check exposing additional information regarding the visitor such as a history of violence, drugs, theft, etc. This added information provides facilities with added peace of mind or instant awareness.

What are the typical concerns from a security standpoint?

Security personnel are concerned about protecting their people, physical property/assets, or intellectual property.

- It is estimated that 1 in 4 in the US has a criminal record

- 49% of data breaches are the result of a lost or stolen device, 16% of those are caused by an outsourcer

- 70% of violent felons had a prior arrest record

- 95% of all companies are victims of theft, only 10% every discover it

Is this legal, and does a facility have the right to scan visitors and refuse access?

Businesses are within their rights to establish their own rules for admitting or banning people from the property – similar to putting a visitor through a bag check or metal detector. The information that FedCheck is accessing is all open source. It is important to note that FedCheck is not intended to be used for public access, paid access, or employees.

How are you accessing the data?

We have written various interfaces to provide a comprehensive search to 2,200 + domestic and international databases with a single query.

Other VMS providers offer a "watchlist query" how is this different?

When looking to maintain a secure facility, FedCheck is much more comprehensive. FedCheck does query watchlists or sanctioned/banned lists, including OFAC, terror watchlists, I NTERPOL, healthcare sanctions, etc. across the globe. FedCheck is unique because it also queries criminal history, arrest records, courts records, and wanted files.

Can we use this as an employee background check?

FedCheck cannot be used as a condition of employment, and therefore cannot be used to replace an employee background check. FedCheck can be used to screen visitors, contractors, and/or temporary workers. Because FedCheck is not being used as an employee background check, it does not fall under FCRA regulations.

How does the FedCheck query work?

FedCheck searches over 2,200+ databases, which includes sex offenders, arrest records, court records, watch lists, sanctioned/banned lists, etc. Within those databases, exist over 1,600 different offense codes, all of which are systematically categorized by the system in real-time. When a query is made, FedCheck uses a proprietary algorithm to search, dissect, and collate the most relevant information and presents the result to the user into 6 distinct categories (Sirens). These 6 distinct Siren types can be turned on or off by the user. Subcategories also exist within the 6 siren types allowing the users can further fine-tune the data by ignoring certain offense types or sources with the 6 categories. For example, if you do not care about traffic offenses, turn them off. Or if you only want to see violent crimes, you can do that as well. Best of all, users can filter offenses by date.

What are the filtering options?

The information queried through Fed-Check can be filtered (toggled on/off) through the following categories and subcategories:
- Wanted Person
- Criminal History
    Violence
    Drugs
    Delinquency/Mischief
    Theft/Burglary
    Neglect/Endangerment
    Vehicle/Traffic
- Terrorism Watchlist
- Arrest Record
    Violence
    Drugs
    Delinquency/Mischief
    Theft/Burglary
    Neglect/Endangerment
    Vehicle/Traffic
- Sex Offender
- Sanctioned/Banned
    Financial Sanctions
    Government Sanctions
    Professional Organizations
    HealthCare Sanctions
    Athletic Sanctions
    Gaming/Casino Bans

The user can also determine how far back in time they want to query to include records from 5 years ago to all-time.

How is this different than a background check?

FedCheck is very similar to background check because we are searching very similar datasets, but there are some small functional and process differences in the way this data is gathered and presented.

As opposed to a traditional employment background check, FedCheck is instant, the data is clean, and the search customizable. This provides immediate actionable intel that allows users to make on the spot decisions.

FedCheck does not check any consumer reporting data as part of the check. FedCheck also cannot be used as a condition of employment. Because of these aspects, a FedCheck query does not fall under FCRA guidelines, whereas a background check would. With a typical background check, the information being gathered must be verified and depending on the location of information, this can be a manual process and could take days to complete. Because FedCheck does not fall under FCRA guidelines, we are not required to verify the information gathered from the return, because of this we can present and instant return.

What kind of data are you getting in my area/state?

Hitting over 2,200 databases, the data gathered from FedCheck is very comprehensive and includes data from each state. FedCheck is not meant to utilized for a single, specific, data source, rather FedCheck provides the ability to quickly search a massive amount of data and instantly receive a readable return – this provides a true digital footprint of the visitor.

Note: Just because a particular city or county agency doesn't provide records doesn't mean we won't be able to access the record, we may still get the record just from a different source. For example, if a city PD doesn't provide criminal history, we may be able to get that information from the county court, or we may get that information from a state database, etc.

If there is a hit, do I have to deny that person?

We do not dictate the policy of any facility. It is up to the discretion of the facility to deny or grant access to a visitor. We want to present actionable intelligence in real-time so security teams can have immediate situational awareness and make a decision for entry. Some facilities may choose to simply allow or deny. Others may grant limited access or require accompanied access. It is our purpose to simply provide the data in the quickest, cleanest, and most relevant manner possible

Who determines whether or not access is given?

The details of the return are not shared with the person scanning the visitor, therefore access determination is typically done "back of the house" by facility personnel that has access to review the return. We do not dictate the policy of any facility; we simply provide the information.

What do you do if someone challenges the result?

If the visitor challenges the result or pushes back, we recommend referring them to local law enforcement.