

CASE STUDY

Gaming Response, Socially Beneficial

The Challenge

The social impact of problem gambling is undeniable as governments all over the world have been implementing significant gambling reforms to minimize gambling harm on communities. A great example being, self-exclusion and third-party barring options measures offered by the South Australian Government, where individuals can ask to be barred or families can request to bar a family member from many forms of gambling such as gaming venues and casinos. Despite the great initiative and strong society's adherence, gaming venues and governments have been struggling to identify barred people in a real environment as manually monitoring for each person of interest was an arduous and inefficient task — which is very difficult without the right video surveillance technology.

To address these challenges, the Government of South Australia has created a new state regulation, which requires an authorized facial recognition solution to be installed in all venues with 30 or more gaming machines, if one or more of which uses note acceptors, because of its ability to quickly identify barred patrons and automatically notify matches to surveillance staff. As a result, gaming venues' authorized security team would have a better chance to enforce gambling bans in gaming venues before a gambler had a chance to cause harm to himself or to his family.

SAFR Solution

SAFR from RealNetworks, was approved by the Government of South Australia as an official facial recognition solution for enforcing gambling bans in gaming venues across the state.

Hotel groups operations managers have been working worked to choose a reliable facial recognition software that is internationally recognized and approved by the SA Government, with an accuracy rate above 99.8% for all races. SAFR was tested and selected by one of the biggest hotel groups in SA because it complies with these criteria and also due to its advantages compared to other FR systems evaluated such as superior performance on live video, previous deployments in gaming in the US, the lower total cost of ownership, and local support with solid FR knowledge.



Hotel Group Overview

A Hotel group across South Australia state, which hosts more than 1 million customers a year

Location: Adelaide, SA, Australia

Use case: Ensure compliance with responsible gaming regulations, identifying barred patrons and alerting staff.

Features:

- Surveillance/Watchlist
- Email and SMS notification
- Integration with CBS DB to automatically enroll barred people in watchlist.
- SAFR Central monitoring center 24/7
- SAFR Mobile APP

Effects of Monitoring:

 <600ms

Email/SMS notifications delivery

 99,87%

Accuracy Rate

Ecash worked in partnership with RealNetworks to deploy SAFR in 7 hotels at the Hotel Group gaming areas. SAFR added superior situational awareness across the group hotels, daily detecting thousands of faces, comparing them to a watchlist of barred people, and alerting surveillance staff about potential barred people by Email and SMS.

“The impact to our day-to-day operations has been minimal, the system just works as we were told it would— emails and SMS alerts have been received in less than 60 seconds”
- Hotel Group Operations Manager

The new surveillance technology offers the possibility to increase the barred people recognition rate by automatic detections, showing the benefits of face recognition technology to social change, and helping problem gambling.

How it Works

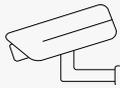
An approved system must offer technical expertise in a large range of capabilities and applications. SAFR has been integrated with the barring database held by the state's CBS (Consumer and Business Services) agency to import and keep barred person data up to date and then use this data to compare with the images of persons entering a gaming area. Furthermore, SAFR action module is used to send SMS and E-mail notifications to the gambling provider when a suspected barred person is identified. Finally, SAFR has been customized to send daily statistics reports regarding the number of persons detected and the number of barred patrons recognized from each gaming venue to SA Government.



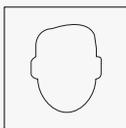
1- Pull Barred People from CBS DB and Create a Unique Face Signature — SAFR/CBS integration is set to automatically sync DBs. The face image is processed, filtered, and converted into a unique face signature comprised of mathematical vectors in Euclidean space derived from over a thousand facial features.



4- Action on Match — If a match is found, the individual is recognized and SAFR sends an e-mail and SMS notification to venue staff in less than 60 seconds.



2- Connect to IP Cameras — SAFR is connected to camera streams by RTSP through the local network.



3- Detect and Recognize faces in live video streams — SAFR detects and tracks multiple faces in each live video stream. Each face image is clipped, optimized, and sent for processing. The detected face is converted into a unique face signature. The resulting signature is matched against the SAFR database, which can compare millions of signatures in near real time

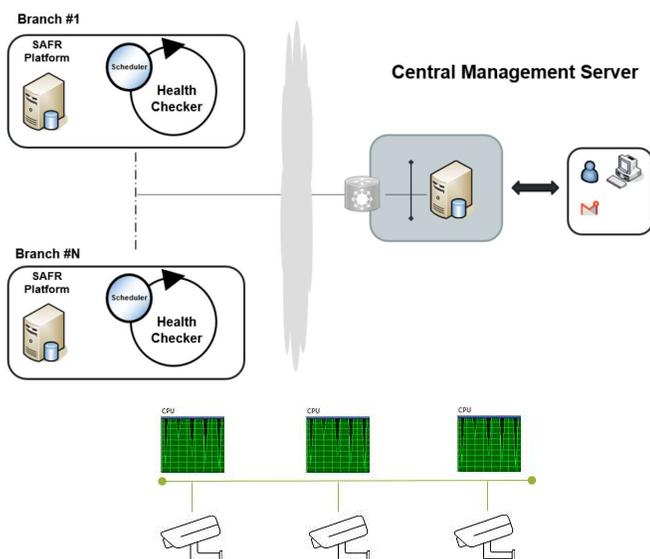


5- Mobile Event Check — Gaming venues staff receives Email and SMS alerts, and a sound alarm on their mobiles to ensure it is seen. All events can be checked using SAFR mobile APP



SAFR Central Monitoring Center

SAFR and Ecash partnership offers server and cameras monitoring 24 hours a day. SAFR health check application runs on each local server, performing a large range of checks such as applications status, camera stream status, system usage with the collection of CPU, GPU, RAM and hard drive stats, ports checks, and CBS connectivity status. Real-time alarm notifications are generated by the central management server when any failures are detected in the system. The SAFR health check solution is self-healing, not only reporting issues, but also taking automatic actions to solve them when any failures are detected.



The screenshot shows the SAFR web interface. At the top, there are navigation tabs: Site, Report, System Usage, App Status, and Camera Feed Status. Below this is a search bar and a table of system status. The table has columns for Time, Company, Site, SAFR ID, IP, Application, Status, and Notify. The table shows several entries with 'Alarm Condition Info' status. Below the table is a 'Video Feeds' section with a 'Feeds by Processor' view. This view shows a list of video feeds with columns for File, Tools, Feeds by Processor, Sort by, Date Added, CPU usage, Address, Last Config, Last Status, and a Configure button. The feeds are sorted by Date Added and show various system components like STANDEVWIN10, argum-MacBookPro11, MSI, LAPTOP-DMGAL7GI, safrlab-Win10, safrlabms-Win10, and safrlab-Micromini.

Choosing a Facial Recognition System That Actually Works

To be approved for use in gaming venues, a facial recognition system must comply with very strict data retention and privacy regulation. SAFR approach to handle data securely provided the baseline to ensure compliance with the SA Government data-sharing agreement. In fact, the SAFR platform is designed, built, maintained, monitored and regularly updated with security in mind. In general terms, SAFR holds only face biometric data, rather than image or personally identifiable data, which can't be reversed to obtain the face image. Moreover, all images and facial data are encrypted using AES256 at rest or in transit, the facial digital signatures are proprietary and not readable by other facial recognition systems. SAFR also offers an on-premise deployment model where ensures that no facial data is ever transported over the internet and flexible data retention policies, which gives complete control over retention. In short, SAFR is able to prevent unauthorized access to use and disclosure of any data collected.



98.85% Recognition Accuracy for Faces with masks



Easily Integrated with Existing Access Control Platforms



95% Mask Detection Rate to Ensure Compliance with WHO Recommendations



Real-time Detection (liveness) and Counterfeit Alerts in Real Time



Touchless Access Control for Masked faces



Occupancy Counting & Mask Detection Dashboard



Better Visibility in Unauthorized Access Attempts



Support for Identity Verification to Prevent ID Card Fraud

PLATFORMS	Windows, Linux, macOS, Android, iOS
ACCURACY	99.87% LFW, 0.0335 FNMR
DETECTION SPEED	~15-60ms @ 30FPS
RECOGNITION SPEED	<100ms per face
TESTED BY	

Secure & Private

SAFR was built with privacy by design principles. All faces signatures and images use AES-256 encryption in transit and at rest, and no data is passed over the internet if SAFR is run on premises.



AES-256
ENCRYPTION

[Learn more at SAFR.com/trust-center](https://www.safmr.com/trust-center)

For more information or to set up a free trial:

[Visit SAFR.com](https://www.safmr.com)

Or contact a SAFR sales representative at:

safmr@realnetworks.com