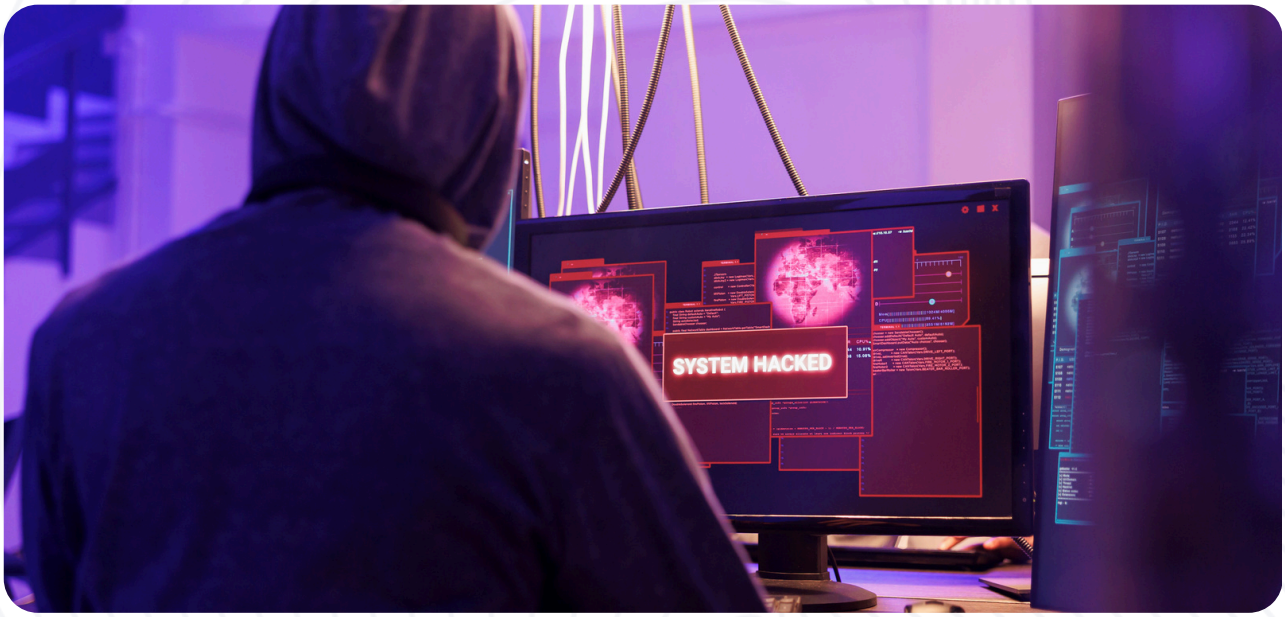
AURAYA

EVA
FORENSICS

Product Sheet

EVA FORENSICS

Mitigate risk of fraudster attacks, reduce friction for customers and agents, reduce the cost of regulatory compliance and enhance brand reputation by better protecting customer data.



Organizations are under increasing attack from fraudsters attempting account takeover and identity theft. Bad actors often mask their real identities using fake or stolen identification or use social engineering techniques to breach an organization's security systems. Once a bad actor finds out how to penetrate an organization, they share the vulnerability with others and repeat the fraud for as long as possible. This magnifies the financial loss, customer inconvenience, regulatory costs, and reputation damage to the organization's brand.

EVA Forensics helps organizations to quickly and efficiently address growing fraud threats. EVA Forensics can run as a standalone dedicated fraud management capability or can be integrated with Auraya's existing solution templates for contact centers and digital channels. EVA solution templates are powered by Auraya's AI powered ArmorVox core biometric engine.

EVA Forensics enables organizations to identify bad actors and take immediate action to thwart fraudulent attempts. Organizations identify bad actors by providing EVA Forensics with voice samples from customer interactions, whether it is during an interaction with an automated service or whilst talking to a call center agent. The audio is compared in near real-time to a group of voiceprints of known bad actors and if the speaker's voice is a match, EVA Forensics alerts the system or personnel to take action.

Importantly, EVA Forensics helps stop fraudulent activity, protect customer data, protect brand reputation, reduce the cost of fraud and provide evidence to enable fraudsters to be prosecuted.

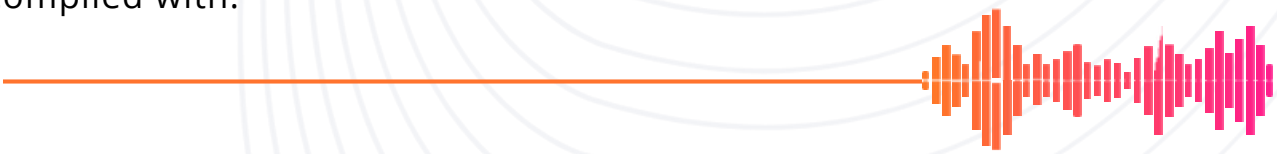
KEY BENEFITS

COST REDUCTION DUE TO ACTIONABLE FRAUD DETECTION AND PREVENTION ALERTS

EVA Forensics reduces the high costs organizations incur when fraud activities are not detected as they are being perpetuated. Real-time alerts enable preventive action to be taken to protect the organization and its customers against attack.

The ability to detect a fraudster whilst they are conversing with a contact center agent or a voice bot not only prevents the direct cost of fraud but reduces the cost of remediating the losses incurred when a customer's identity is stolen or their data is compromised.

EVA reduces the cost of regulatory compliance and can help to reduce the cost of sanctions imposed by regulators when a customer's data is exposed to fraudsters or the Know Your Customer (KYC) elements of the Anti-Money Laundering and Counter-Terrorism Financing Act (AML) are not complied with.



IMPROVED FRAUD DETECTION AND INVESTIGATION

EVA Forensics enhances fraud detection with advanced voice-matching capabilities and support for text-independent voiceprints, allowing organizations to identify threats with greater precision. The addition of automated noise removal during bulk audio imports and better voiceprint organization simplifies the investigation process, saving time and resources.

OPTIMIZED SYSTEM PERFORMANCE AND EFFICIENCY

With improved computational efficiency and enhanced scalability, EVA Forensics ensures seamless operation under high workloads. The system adapts to organizational needs, delivering reliable performance while reducing resource costs.

IMPROVED CUSTOMER AND AGENT EXPERIENCE

When an organization is effectively preventing fraudsters from accessing customer accounts, then organizations can choose to reduce the identity verification burden on each legitimate customer interaction making the customer interaction journey more convenient and pleasant for both the agent and the customer. Better experience for customers and agents drive improved loyalty and customer retention and brand value.

IMPROVED REGULATORY COMPLIANCE

With EVA Forensics, organizations can use voice biometric AI to help reduce the regulatory costs associated with non compliance with anti money laundering (AML) and know your customer (KYC) and data privacy legislation. EVA Forensics allows organizations to take corrective actions when a person tries to create multiple accounts online using stolen identification documents or a known bad actor is identified during an automated or phone based customer onboarding process. EVA Forensics can also be used to scan all customer voice records against every other customer to identify an individual who may have multiple identities. This identification of potential duplicate identities can be used proactively to manage KYC compliance issues and account phoenixing.

IMMEDIATE BENEFITS WITH FAST AND FLEXIBLE DEPLOYMENT

EVA Forensics is provided as a solution template allowing organizations to deploy the solution within their cloud service or on-premise IT infrastructure ensuring all customer data is retained within the organization's secure infrastructure. No data leaves the organization control for any reason.

There is no requirement to enroll an organization's customer voiceprints to start experiencing the benefits. EVA Forensics allows organizations to create the voiceprints of known identities and other persons of interest using historical recordings. Permission to use audio of known bad actors is not required if the purpose is to detect and prevent fraud.

Once the voiceprints of identities are enrolled, organizations can simply use the audio from customer interactions to check to see if their voice matches any enrolled voiceprints. In its simplest form, EVA Forensics can be created in an organization's secure AWS cloud service, and, using cloud formation tools, can start delivering fraud detection and prevention capabilities within hours.

An organization's in-house or existing outsourced IT and fraud team can be accredited to deploy and start using EVA after a 3-day onboarding workshop. Alternatively, Auraya has a global network of accredited integration and support partners that can assist in deploying and supporting EVA Forensics solutions.

SEAMLESS AUTO-SCALING CAPABILITIES FOR SMALL AND LARGE ORGANIZATIONS

With consumption-based licensing and infrastructure costs scaling from a few thousand dollars per annum, EVA Forensics can be switched on to solve fraud issues for small organizations or as a point solution within a large organization. With the auto-scaling capabilities, organizations can start small and expand or they can simply turn it on across the entire enterprise. Integration to multiple on-premise and cloud-based contact centers is achieved simply with open APIs, enabling integration and customization to meet any organization's requirements.

VERIFY IN ALL CHANNELS USING THE SAME VOICE BIOMETRIC ENGINE

EVA Forensics can be integrated with Auraya's suite of EVA solution templates.
EVA Web solution template provides secure, yet convenient speaker recognition for chat, messaging, websites and applications. Simply activate EVA Web as a secure factor from Auth0, PingFederate, Okta, or your preferred identity and access management platform.

EVA Contact Center solution templates deliver an enterprise-wide voice biometric solution for contact centers. Active and passive enrolment and verification capabilities are designed to improve personalized self-service and more efficient and helpful agent interactions.

The complete EVA suite adds voice biometric speaker recognition to both telephony and digital channels. EVA improves customer and agent experience, reduces costs, and improves an organization's ability to deliver a delightful and personalized customer experience whilst identifying and enabling real-time action to protect against bad actors.

KEY FEATURES

ENROLL VOICEPRINTS FROM VARIOUS SOURCES

Enroll Fraudster and Serial Harasser Voiceprints from Historical Call Recordings

EVA Forensics allows organizations to enroll the voiceprints of bad actors and repetitive harassers from historical call recordings. Most organizations have archives of call recordings from agent conversations that were later identified as a fraud event. This archive of known fraudster recordings is used to create the initial identity voiceprint group in EVA Forensics. The recordings that are used to create voiceprints are automatically treated by EVA Forensics to remove non-voice audio such as on-hold music, dial tone, and silence as well as the agent side of the conversation. This means that recordings from both inbound and outbound calls can be used to create voiceprints.

Organizations can also use historical call recordings from other organizations to combat fraud across an industry or in a specific region. Organizations utilizing EVA Forensics can acquire and share the voice files of known bad actors with other organizations and enrol voiceprints from this pool of shared information. This protects organizations from known fraudsters who have yet to target and attack them.

Enroll Fraudster Voiceprints via Audio Recordings from IVR Interactions that Were Later Found to be Fraudulent

If an organization has been recording audio from an IVR or voice bot interaction, then any audio captured during these interactions that were later found to be fraudulent can also be used to create an identity voiceprint.

Enroll New Customers from Recordings of Audio from Browsers, Chat, and Agent Conversation During New Customer Onboarding

EVA Forensics can automatically create voiceprints that allow all new customers (activators) to be compared with other recent activators which help organizations detect when one bad actor tries to create multiple new accounts with only one voice.

Enroll Audio Automatically from Suspicious Activity

Organizations can capture audio from IVR, voice bot, and agent conversations where the activity of the caller indicated fraud attempts.

For example, if a caller tried to access a person's account using social engineering techniques only to be thwarted by the contact center agent, then the audio recording of that conversation can be used to add a voiceprint to a "Suspected Identities" group. Similarly, if a person is detected trying to log into a voice biometrically protected account and the biometric match indicates that the person is not the legitimate customer then the audio from the failed attempt can be compared to the "Known Identities" group for match analysis. If the voiceprint is not a match to a known identity then this new suspicious audio can be used to create a new "Suspected Identity" voiceprint.

Enroll Synthetic Voice Generators and Voice Disguising Devices

Fraudsters may use technology that disguises their voice when they attempt fraud with a call center agent, EVA Forensics can enroll any number of voice disguising technologies or even the latest versions of synthetic voice generators, and these "voice synthesizer’" models can scan all other conversations to identify when a person tries this technique.

CURATE FRAUDSTER VOICEPRINTS TO IMPROVE PERFORMANCE

EVA Forensics provides fraud analysts with a range of tools to compare known fraudster recordings to detect multiple recordings from the same fraudster. If the same fraudster appears on multiple recordings then the additional recordings can be combined to create a stronger voice print which improves the ability of EVA Forensics to detect that voice in any future conversation.

CUSTOM GROUPS AND ALERTS

With EVA Forensics, organizations can create custom groups to organize and manage the stored voiceprints. Organizations can organize the voiceprints to different groups such as "Persistent Harassers" and "Recent Activators". Having multiple smaller groups to crossmatch improves the accuracy of receiving a positive match without triggering false flags.

Organizations can also issue special alerts and workflows for each custom group, allowing the organization to implement relevant measures when a crossmatch returns a positive match.

For example, agents can implement more stringent measures when a crossmatch returns a positive match from a "Known Identities" group and a more cautious approach when a crossmatch returns a positive match from a "Suspected Identities" group.

FORENSIC ANALYSIS TOOLS

EVA Forensics provides a powerful suite of analytic tools to help fraud analysts to listen to suspect calls. Any call can be listened to whilst watching a Spectrum Analyzer. Sections of calls can be zoomed into and irrelevant audio can be removed. Call records being analyzed can contain any relevant metadata to help the fraud analysis professional build a complete picture of the event. EVA can display several different scores indicating the likelihood of a match with an enrolled voiceprint. Scores include Raw Score, Imposter Probability Score (cumulative density function) and Odds Score (probability density function).

DATA RETENTION AND SECURITY

EVA Forensics securely logs all activity, including original audio, metadata, and changes made by analysts, ensuring a clear chain of custody for potential prosecutions. Access is protected with role-based controls, SAML2 authentication, and voice biometric verification, with additional security details available for authorized personnel.

REAL-TIME AND SCHEDULED CROSSMATCHING OF CANDIDATE CONVERSATIONS AGAINST GROUP OF VOICEPRINTS

EVA Forensics can process over 125 million crossmatches per hour on a single server. With automatic scaling, EVA Forensics can provide real-time alerts if a suspicious or known bad actor is identified in any audio provided to EVA Forensics.

EVA scales to match any load conditions, which means that EVA can crossmatch candidate calls across all existing EVA groups and look for match scores that signal a likely match with one of the enrolled identities.

Auraya Systems Pty. Ltd.

Auraya is a voice intelligence company with the mission of empowering people and organizations to interact and engage with convenience and security in all channels and languages. Auraya develops next-gen voice biometric AI technology to deliver easy-to-use and highly secure speaker recognition and fraud detection capabilities. Auraya provides its technology to a global network of partners who incorporate Auraya's voice biometric technology into their secure, customer-facing applications and fraud detection solutions. The ecosystem of partners delivers solutions in all industries including government, education, healthcare, financial services, retail services, and telecommunications. If you would like to talk to the team at Auraya, send us an email at info@aurayasystems.com.

AURAYA

394 Lane Cove Road, Macquarie Park, NSW 2113, Australia

info@aurayasystems.com

aurayasystems.com

Australia | United Kingdom and Europe | Americas | New Zealand | Asia