VERINT

Protecting Sensitive Information with Advanced AI and Analytics

V

Table of Contents

Introduction

The proliferation of channels for interacting with customers along with new and frequently changing laws regarding the protection of personally identifiable information (PII) and Payment Card Industry (PCI) standards make the protection of that sensitive information an ongoing challenge. The growth in the number of employees working remotely has also led to increased security concerns and challenges when it comes to handling sensitive personal information.

One of the challenges to meeting privacy regulations and government or industry regulations is accurately identifying interactions containing PII and PCI. PII is any data that can be used to identify a specific individual. This includes information such as names, addresses, social security numbers, and date of birth which is often collected during the verification process or when updating customer information. PCI refers to credit card information, such as credit card numbers, card verification values (CVVs), and expiration dates.

VERINT. The Customer Engagement Company® \ 3

Verint Da Vinci's Advanced AI Advantage

With the Verint® Da Vinci™ PCI Interaction Redaction Bot, sensitive PII data can be removed or masked so that it cannot be accessed by anyone without specific permission. Powered by Verint Da Vinci AI, Verint Da Vinci Redaction can:

- Remove PII from call transcripts.

- Remove PII from textual interactions

- Suppress audio during playback

- Support redacted audio and transcript exports (based on permissions)

- Apply redaction on bulk recordings
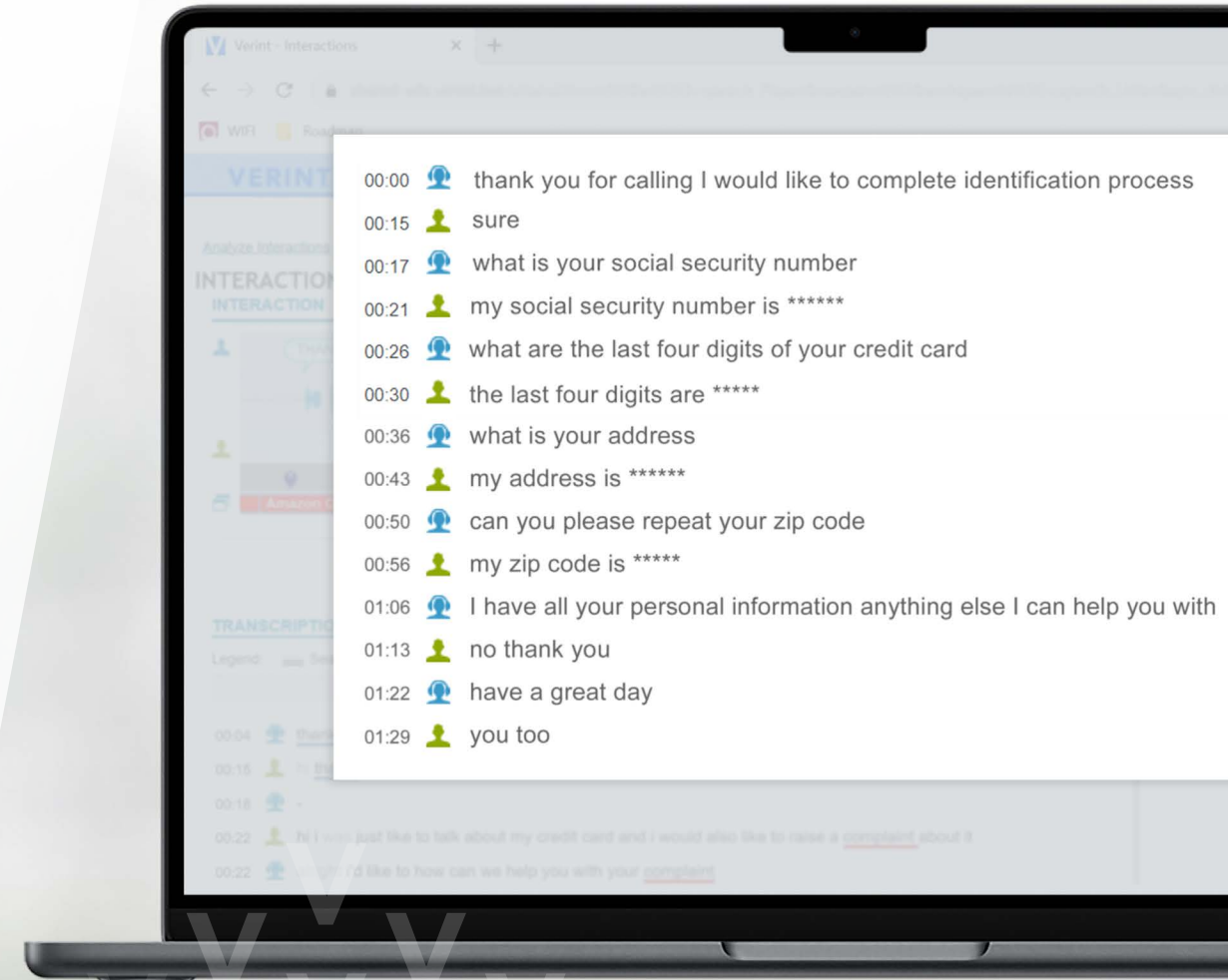
Benefit from Real-Time and Post-Call Redaction

—

Real-time Redaction Driven by DPA

Using Verint Desktop and Process Analytics™ (DPA), automatic triggers can pause call recording when sensitive information is being shared — preventing it from being captured so there's no risk of it being exposed to any unauthorized individuals — and then resume the recording when PII is no longer being discussed. This approach is ideal when an organization wants to completely remove PII data from transcripts and recordings.
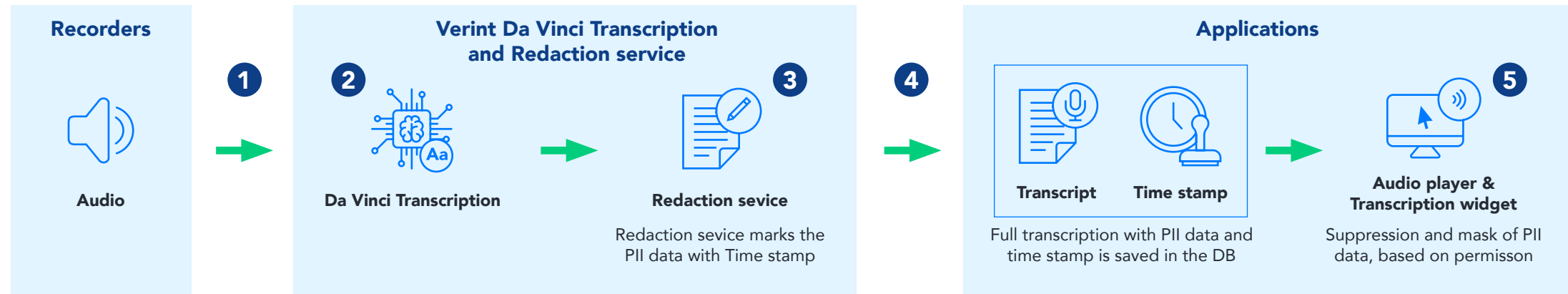
Post-Call Redaction Driven by AI

With post-call redaction, the entire call is captured, but once the call is recorded and transcribed, PII is removed from the transcript. In addition, the audio file is disabled for those without express permission to access it. While the redacted transcript is being created, recordings are automatically tagged with mask and unmask points to indicate where the content is redacted, and a redacted audio file is also created. At playback, only individuals with an elevated privilege are able to replay the entire recording.

Verint Da Vinci Replay Redaction can be used by itself, or in conjunction with Verint Desktop and Process Analytics for an extra level of protection with two layers of redaction.

VERINT The Customer Engagement Company®

Additional Redaction Capabilities Provide Flexibility

PII Redaction Bot - Flow

Recorders

Audio

Verint Da Vinci Transcription and Redaction service

1 **2** Da Vinci Transcription

3 Redaction sevice

Redaction sevice marks the PII data with Time stamp

4

Applications

Transcript   Time stamp

Full transcription with PII data and time stamp is saved in the DB

5 Audio player & Transcription widget

Suppression and mask of PII data, based on permisson

Redaction for Post-Call Protection of PII

What about redaction options for companies that aren't using Verint recording capabilities but want to apply speech analytics to their recordings while ensuring the unified player doesn't expose PII? Or companies that have historical recordings that were made without Pause and Resume but now want to export those recordings for analysis while hiding PII from anyone without proper permissions?

In this case, audio that was recorded by third-party recorders can be ingested into Verint Platform. Verint's transcription and redaction process can be applied as if the audio was captured by Verint Recording and achieve the same results and functionality.

Conclusion

The redaction of PII helps ensure against the misuse or abuse of personal information through identity theft, fraud, and other forms of cybercrime. Organizations that fail to protect their customers' sensitive data run the risk of legal actions, hefty fines, the loss of customer trust and damage to their reputation.

By implementing strong safeguards and guidelines, governments and regulatory bodies hope to minimize the risks associated with the collection, storage, and use of PII and promote greater transparency and accountability among businesses and organizations that handle such data. With the continued rise in the numbers of data breaches and cyberattacks, it is likely that new rules and guidelines for the collection, storage, and use of PII by businesses and organizations will continue to be enacted globally.

Verint Da Vinci Redaction helps safeguard organizations like yours to ensure your customers' sensitive personal information is protected from exposure to unauthorized access while keeping your company safe from the negative impacts of the exposure of personally identifiable information.

VERINT

The Customer Engagement Company®

Americas

info@verint.com

+1-770-754-1900

1-800-4VERINT

Europe, Middle East & Africa

info.emea@verint.com

+44(0) 1932 839500

Asia Pacific

info.apac@verint.com

+(852) 2797 5678

---

verint.com

x.com/verint

linkedin.com/company/verint

verint.com/blog