Example of Microsoft 365 Document Fingerprinting

# Introduction

Document fingerprinting in Microsoft 365 allows you to create unique identifiers for documents based on their contents. This helps in identifying sensitive information and ensuring proper data governance. Fingerprinting can be used to match documents containing sensitive data with predefined sensitive information types.

# Example Setup

Here we demonstrate how Microsoft 365 uses document fingerprinting for identifying sensitive content, like Personally Identifiable Information (PII) or financial data. We will use an example document containing the following types of sensitive data: Name, Address, Credit Card Number.

# Example Document Content

John Christopher  
1234 Maple Street  
New York, NY 07008  
Credit Card: 4111 1111 1111 1111

# Fingerprint Configuration

To configure document fingerprinting, you will need to create a sensitive information type in Microsoft 365 Compliance Center. After creating the fingerprint, apply it to relevant documents. Microsoft 365 will then analyze the content and generate a unique fingerprint for this document based on the data included.

# Fingerprint Example Description

For the document containing sensitive data such as 'John Doe' and '4111 1111 1111 1111', Microsoft 365 generates a unique identifier based on the content. If a document with the same content is uploaded in the future, Microsoft 365 can match the fingerprint and enforce any necessary data loss prevention (DLP) policies.

# Conclusion

Document fingerprinting provides an effective method for identifying and managing sensitive data within your organization. Once set up, this feature can help prevent unauthorized sharing of sensitive content and ensure compliance with data governance policies.