Exposure Data Audit

Locating Personally Identifiable Information (PII) in SQL Server

Alan Faulkner

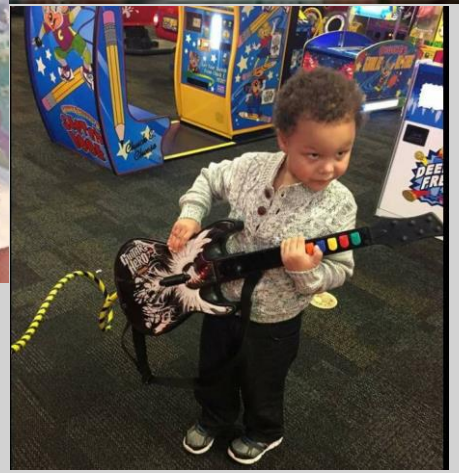
- Principal Consultant – Pragmatic Works
- Speaker, SQL Saturdays, Code Camps, Webinars, PreCons, 24 Hours of PASS
  - Generally speaks about living in a van down by the river.
  - Likes BBQ
  - Will work for cupcakes
- previously - professional rock guitarist & now - aspiring Flamenco guitarist

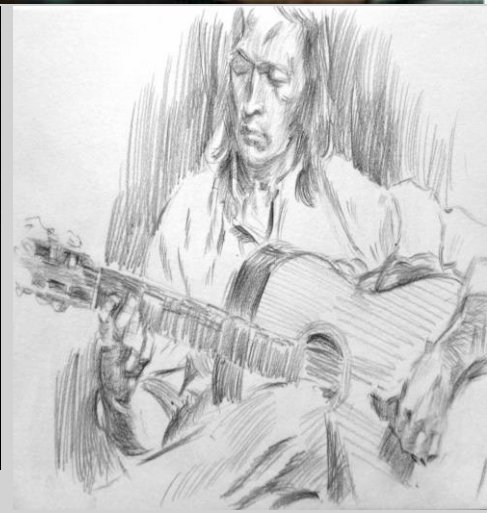
@FalconTekNic

www.linkedin.com/in/alandfaulkner

http://falconteksolutionscentral.com

afaulkner@pragmaticworks.com





PII – What is it?

- Information that can be used to distinguish or trace an individual's identity.
- Name (e.g. Mother's Maiden Name)
- Social Security Number
- Date and Place of Birth
- Linked to an individual – medical, educational, financial, employment

Records of 340 million consumers reportedly exposed

Recent Data Leak Exposed Information of 123 Million American Households

"Our investigation has determined that approximately 3.4 million unique payment cards were used on the impacted POS terminals during this period. "

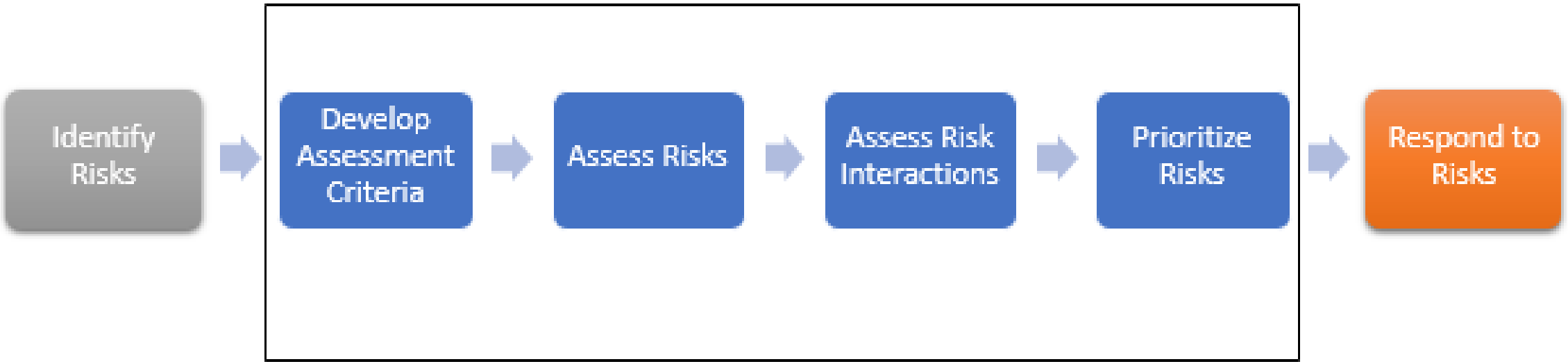
Exposure Data Audit Solution

- 3-Part Solution
  - Database/T-SQL
  - SSIS
  - PowerBI
- Risk Rating Scale
- Leverage the information collected to identify possible next steps.

Consequence Value (CV)		Impact to…				
Rating	Value	Personnel Safety	Resources	Work Performance	Property Damage	Reputation
No Risk	1	No injuries	No Impact	No Delays	Minor	No impact
Minor	2	Minor injuries	Moderate impact	Modest Delays	Moderate	Potential damage
Moderate	3	Moderate to life impacting injuries	Additional resources required	Significant delays	Substantial	Damaged
High	4	Life threatening injuries from single exposure	Institutional resources required	Major operational disruptions	Severe	Loss of Confidence

Microsoft® SQL Server® Integration Services

Exposure Data Audit Process Flow



Demo - Exposure Data Audit Solution

- Review of DB Project Visual Studio
- Review of SSIS Project/Package (Visual Studio)
- Review of PowerBI Solution

Consequence Value (CV)		Impact to...				
Rating	Value	Personnel Safety	Resources	Work Performance	Property Damage	Reputation
No Risk	1	No injuries	No Impact	No Delays	Minor	No impact
Minor	2	Minor injuries	Moderate impact	Modest Delays	Moderate	Potential damage
Moderate	3	Moderate to life impacting injuries	Additional resources required	Significant delays	Substantial	Damaged
High	4	Life threatening injuries from single exposure	Institutional resources required	Major operational disruptions	Severe	Loss of Confidence

Microsoft® SQL Server® Integration Services

Exposure Data Audit Discoveries

- Memory Optimized Data

Msg 41317, Level 16, State 6, Line 137
A user transaction that accesses memory optimized tables or natively compiled modules cannot access more than one user database or databases model and msdb, and it cannot write to master.

- Binding Errors

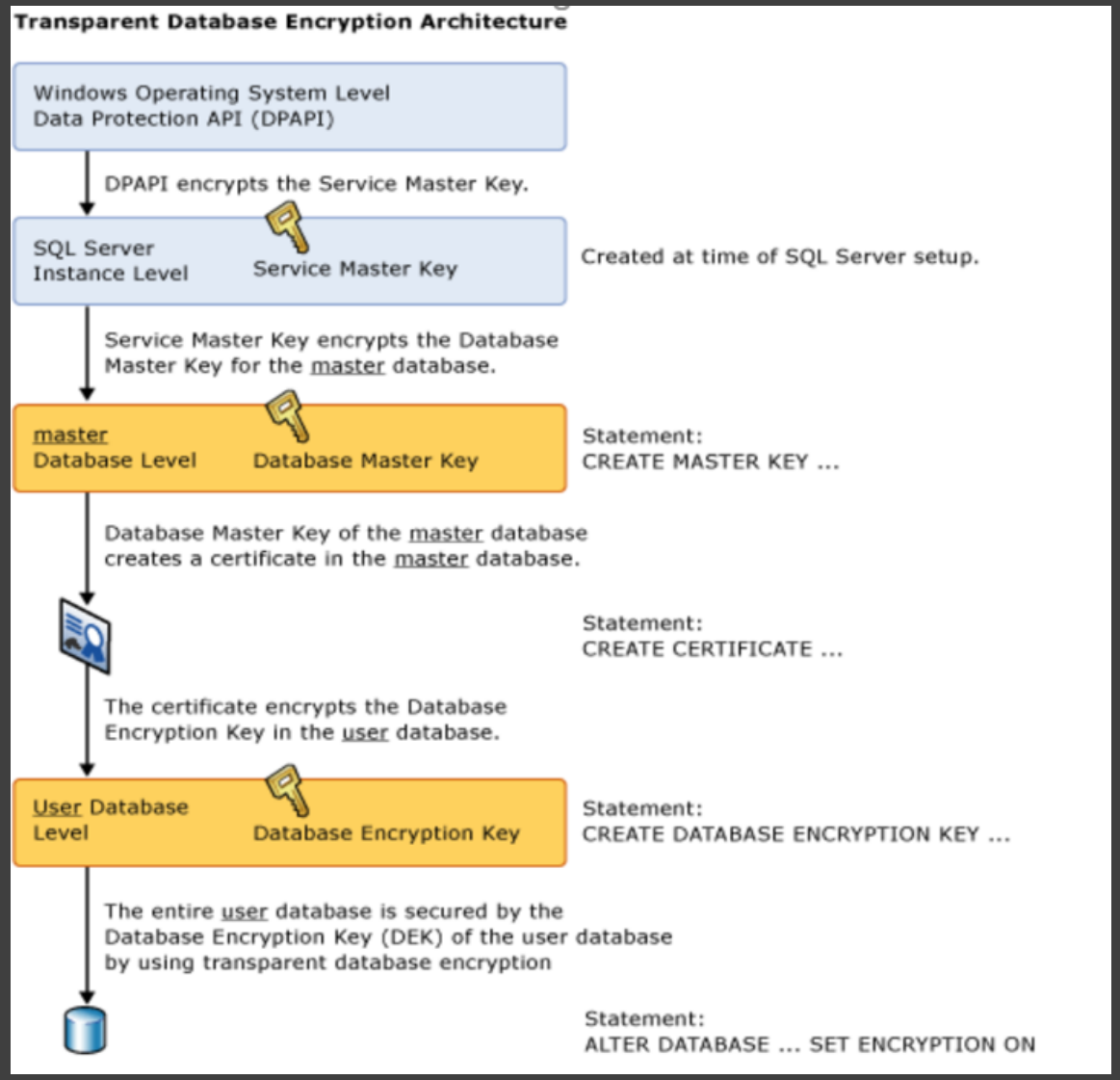
```
CREATE DATABASE [WideWorldImportersDW]
 CONTAINMENT = NONE
 ON  PRIMARY
( NAME = N'WWI_Primary', FILENAME = N'C:\Program Files\Microsoft
SQL Server\MSSQL13.SQL2016\MSSQL\DATA\WideWorldImportersDW.mdf' ,
SIZE = 2097152KB , MAXSIZE = UNLIMITED, FILEGROWTH = 65536KB ),
 FILEGROUP [USERDATA]  DEFAULT
( NAME = N'WWI_UserData', FILENAME = N'C:\Program Files\Microsoft
SQL
Server\MSSQL13.SQL2016\MSSQL\DATA\WideWorldImportersDW_UserData.n
df' , SIZE = 2097152KB , MAXSIZE = UNLIMITED, FILEGROWTH =
65536KB ),
 FILEGROUP [WWIDW_InMemory_Data] CONTAINS
MEMORY_OPTIMIZED_DATA  DEFAULT
( NAME = N'WWIDW_InMemory_Data_1', FILENAME = N'C:\Program
Files\Microsoft SQL
Server\MSSQL13.SQL2016\MSSQL\DATA\WideWorldImportersDW_InMemory_D
ata_1' , MAXSIZE = UNLIMITED)
 LOG ON
( NAME = N'WWI_Log', FILENAME = N'C:\Program Files\Microsoft SQL
Server\MSSQL13.SQL2016\MSSQL\DATA\WideWorldImportersDW.ldf' ,
SIZE = 495616KB , MAXSIZE = 2048GB , FILEGROWTH = 65536KB )
GO
```

SQL Server 2016 – Data Security

- Transparent Data Encryption
- Always Encrypted
- Row Level Security
- Dynamic Data Masking

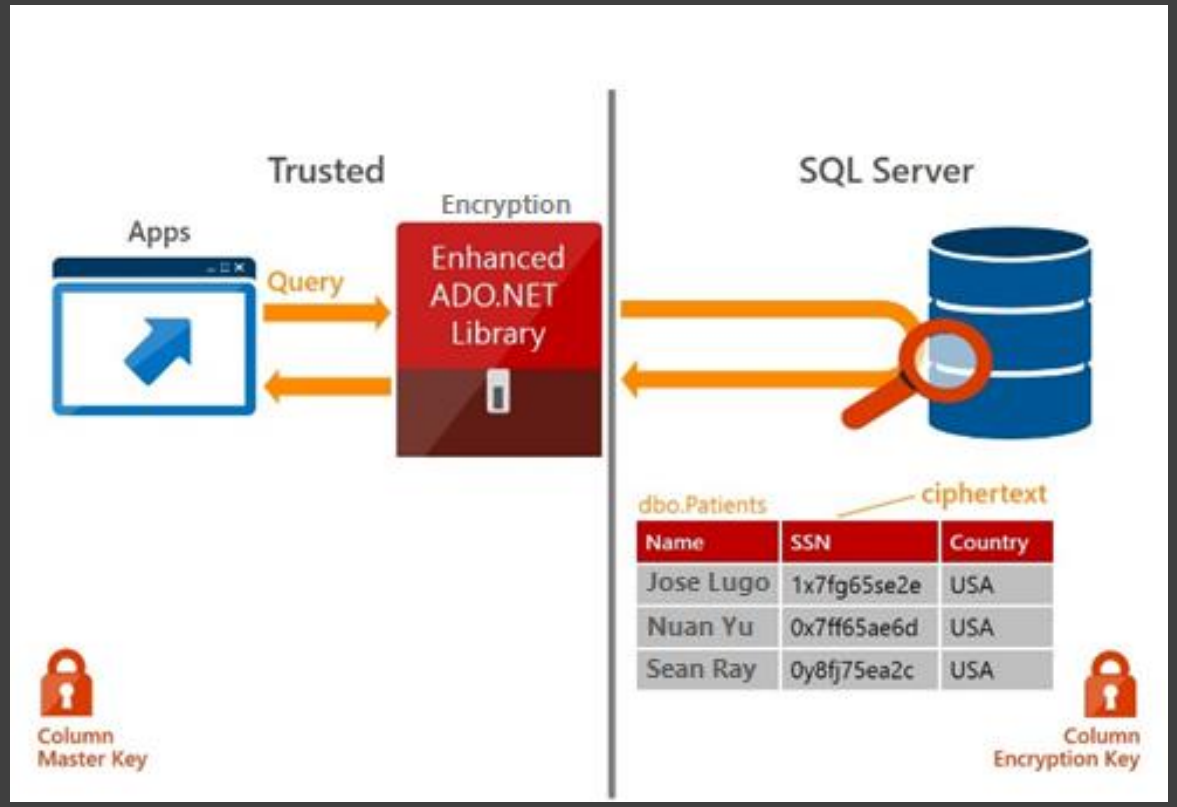
Transparent Data Encryption - Overview

- Encrypts Data on Media
- Secured via Encryption Key
- Encrypts data at rest-not in flight



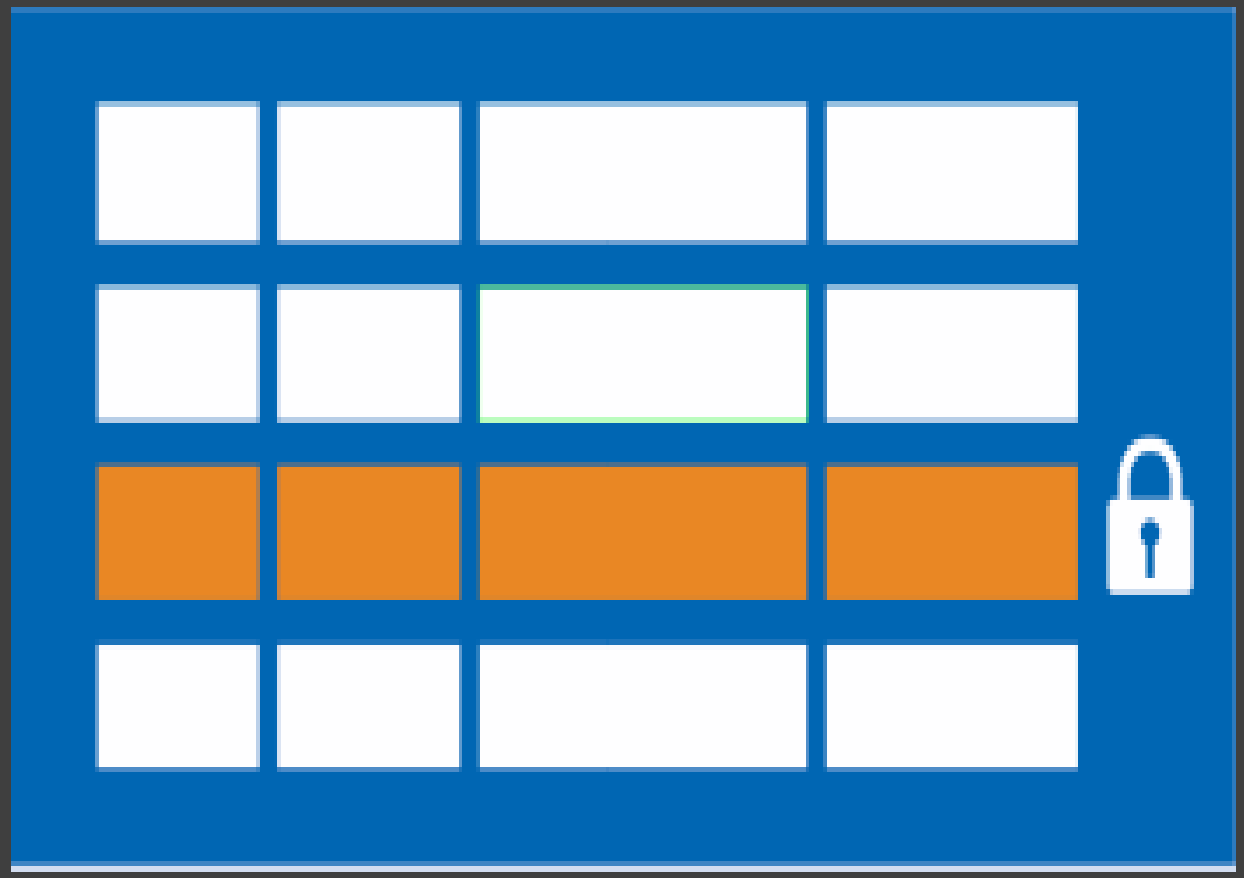
Always Encrypted - Overview

- Protects data in flight & at rest
- Deterministic vs Randomized Encryption
- Use Cases
  - Client and Data On-Premises
  - Client On-Premises Data in Azure
  - Client and Data in Azure



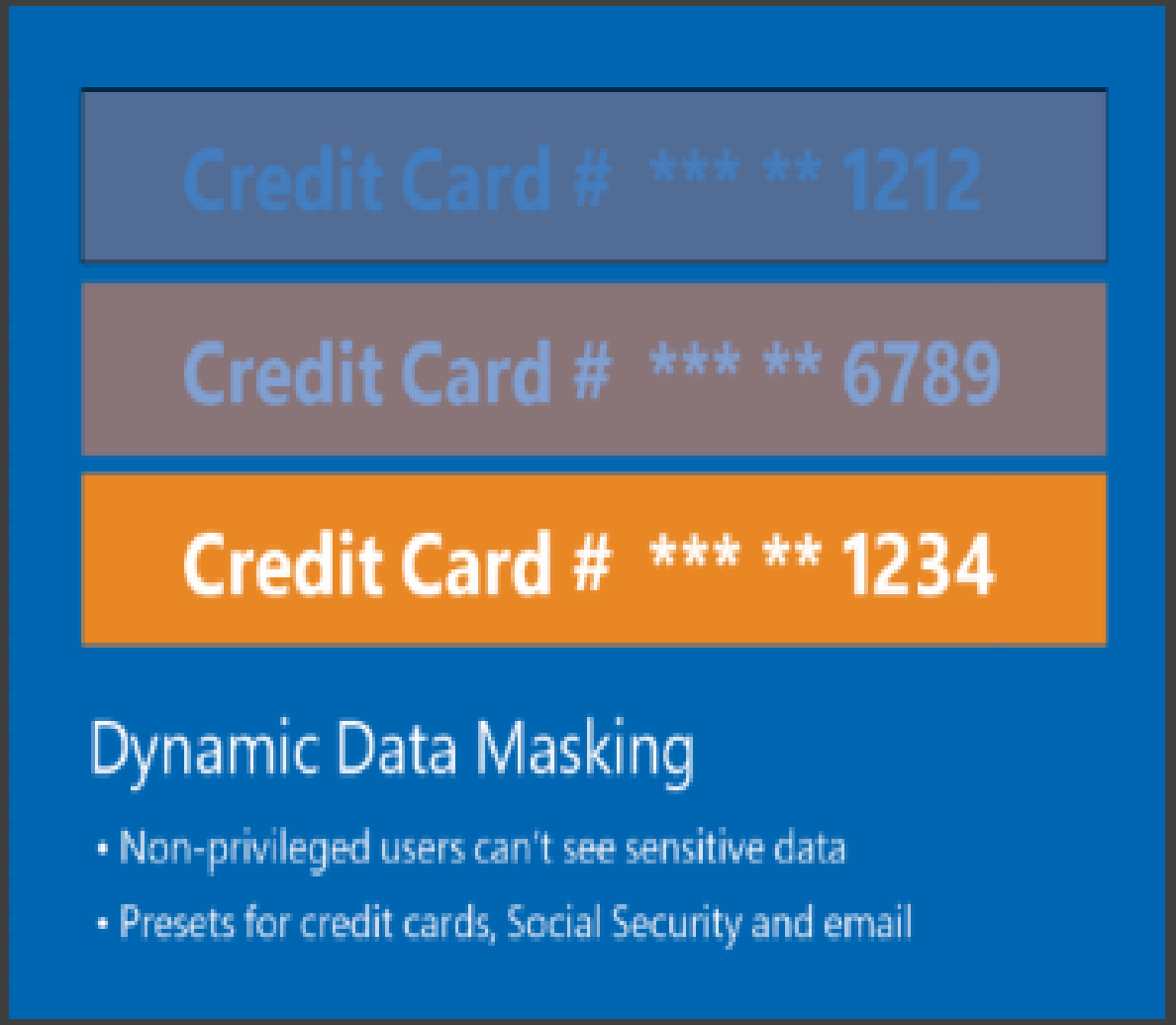
Row Level Security - Overview

- Controls access to rows based on user characteristics
- Restriction logic located in database tier
- Use Cases
  - Hospital
  - Bank
  - Application



Dynamic Data Masking - Overview

- Limits sensitive data by masking to non-privileged users
- Designate how much of the sensitive data to reveal
- Can be used in conjunction with auditing, encryption, and row level security
- Use Cases
  - Masking PII Data (e.g. SSN, Credit Card Number)




Questions?