WHAT’S AT STAKE?

- **September 2018**
  - **Uber**
  - **US FINES: $148M**

- **January 2019**
  - **Google**
  - **US FINES: $99M**

- **July 2019**
  - **Equifax**
  - **US FINES: $575M**
  - **EU FINES: €50M**

- **July 2019**
  - **British Airways**
  - **GDPR FINES: £183M**

- **July 2019**
  - **Marriott**
  - **GDPR FINES: £99M**

- **July 2019**
  - **Facebook**
  - **GDPR FINES: $5B**
GDPR FINES

Data protection authorities take a top-down approach to calculating administrative fines, starting from the maximum allowed percentage of global turnover, i.e. 4% of a company’s global annual turnover or €20 million – whichever is greater.
AGGRAVATING FACTORS:

• IGNORING WARNINGS
• DELAYING INVESTIGATIONS
• DELEGATING BREACH REMEDIATION
• INADEQUATE DOCUMENTATION
• INSUFFICIENT NOTIFICATION
MITIGATING FACTORS:

• SELF DISCLOSURE
• EXPEDIENT REMEDIATION
• TRANSPARENCY IN REPORTING
• INFRASTRUCTURE & GOVERNANCE ENHANCEMENTS
• PROACTIVE CONTROLS AND COMPLIANCE TESTING
• RISK AND DATA MAPPING

These will help evidence that a breach is anomalous and not down to systemic weakness.
THE BURDEN IS ON THE COMPANY

Until there is more transparency and consistency in the determination of penalties under the GDPR, companies facing enforcement must equip themselves to persuade the authorities of mitigating factors.

Tens or even hundreds of millions could be saved in the future by taking the right mitigating actions today.
FORENSIC INVESTIGATION: CREATING THE NARRATIVE

WHO
WHAT
WHERE
WHEN
WHY
HOW
FORENSIC INVESTIGATION: CREATING THE NARRATIVE

WHO

Identify:

- Bad Actors (if known)
- Impacted Customers
- Relevant Custodians
FORENSIC INVESTIGATION: CREATING THE NARRATIVE

WHO

WHERE

WHEN

WHY

HOW

WHAT

Identify:
- What data was breached, exfiltrated and/or misused
- What data was reviewed in course of the investigation (email, chat, voice, docs)
FORENSIC INVESTIGATION: CREATING THE NARRATIVE

WHO

WHAT

WHEN

WHERE

WHY

HOW

Identify:
- Jurisdictional implications (notification requirements, privacy issues)
Identify:
• Timing of breach/misuse in order to ensure all impacted datasets and customers are accounted for.
Identify:
• Motivations behind the breach/misuse if possible, in order to ensure it is accounted for in risk assessment and control structure moving forward.
Identify:
  • Root cause of security or policy gap, and ensure a feedback mechanism to ensure security/compliance program are bolstered moving forward