

Industry Spotlights Webinar Series: Big Data's Impact on Employers

May 30, 2018

Agenda

1. Big Data Analytics in Hiring
2. Developing and Maintaining a Benefit Plan
Cybersecurity Policy for Participant Data
3. Pay Equity Audits

EPSTEIN
BECKER
GREEN

Big Data Analytics in Hiring

Presented by



Adam S. Forman

Member of the Firm – Detroit/Chicago

aforman@ebglaw.com

248-351-6287



Nathaniel M. Glasser

Member of the Firm – Washington, DC

[nglasser@ebglaw.com](mailto:nklasser@ebglaw.com)

202-861-1863

What is “big data”?

No definitive definition

- “Data of a very large size, typically to the extent that its manipulation and management present significant logistical challenges.” (*Oxford English Dictionary*)
- “An all-encompassing term for any collection of data sets so large and complex that it becomes difficult to process using on-hand data management tools or traditional data processing applications.” (*Wikipedia*)



Broad term encompassing volume, speed, type and deciphering

Synonymous for actual data and computerized analysis



What comprises the “big data”?



Big Data

Publicly available data

- Criminal records, court filings, etc.
- Social media profiles/activity

Applicant-provided data

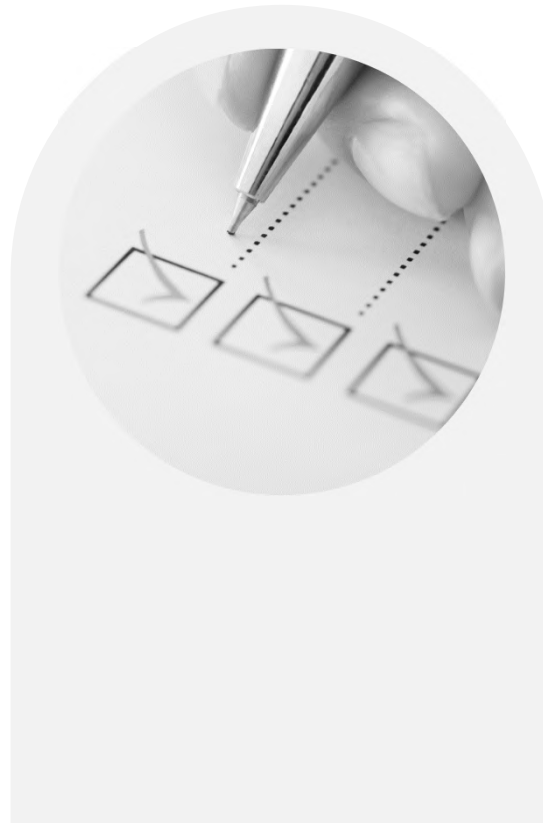
- Resume
- Application information

Employer-stored data

- Employment history
- Performance
- Personality testing and other past assessments

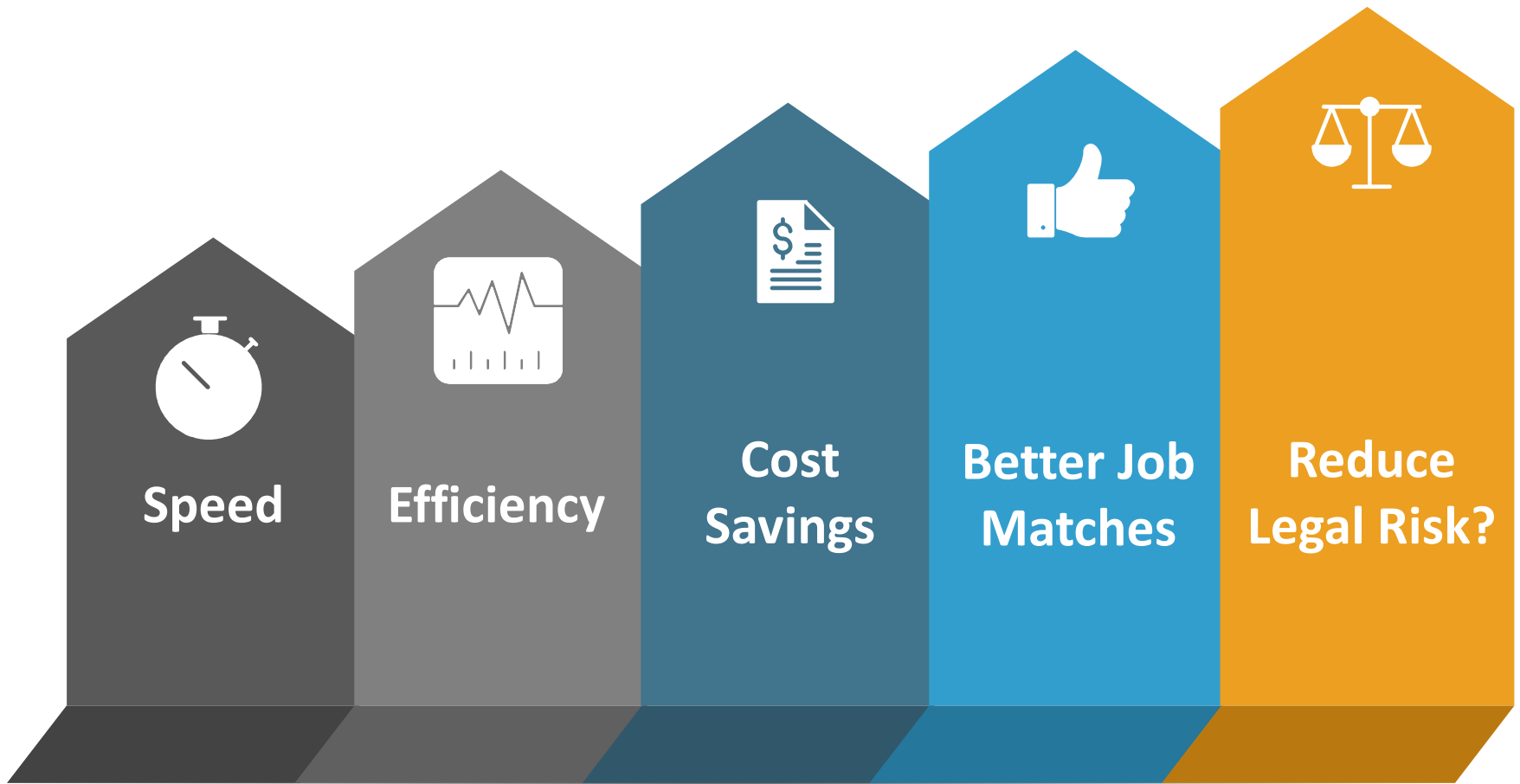
What can big data analytics do for hiring?

- 01 Sourcing and matching functionality
- 02 Screening interviews
- 03 “Statistically proven” screen questions based on “world class behavioral data analytics”



- 04 Automated ranking/scoring
- 05 Personality tests and cognitive assessments, and other tests
- 06 Automated on-line reference checking

Potential Benefits



Potential Drawbacks & Legal Risks

Increased scrutiny from administrative agencies

Disparate Impact

- Facially neutral algorithm
- Class actions / missing “glue”?

Lingering disparate treatment issues

- Encoded Biases?
- Disability Discrimination?

Fair Credit Reporting Act (FCRA)

How to Evaluate These Products

1

Due Diligence on Products

- Data retention agreements – record keeping obligations
- Indemnification agreements
- Auditing agreements

2

Adverse Impact Analysis

- Each time the algorithm is used for decision-making purposes
- Periodic statistical sampling

3

Data Security Protections

EPSTEIN
BECKER
GREEN

Developing and Maintaining a Benefit Plan Cybersecurity Policy for Participant Data

Presented by



Michelle Capezza

Member of the Firm – New York

mcapezza@ebglaw.com

212-351-4774

The Case for Benefit Plan Data Security Policies






A Call to Action



- We live in a Digital World of Big Data and Increasing Inter-Connectedness
- Increasing Cyber Threats
- Data Breaches are a “When” not an “If”
- The Advisory Council on Employee Welfare and Pension Benefits Plans and Retirement Industry Groups have identified many risks in connection with employee benefit plan administration and the need to implement certain safeguards

ERISA Fiduciary Responsibility

To Name a Few of those Responsibilities:

-  Acting solely in the interest of plan participants and beneficiaries with the exclusive purpose of providing benefits to them (duty of undivided loyalty)
 - *E.g.*, ensure timely remittance of employee contributions, maintain plan records, claims procedures, avoid misleading statements and misrepresentations
-  Use plan assets for the exclusive purpose of paying plan benefits or defraying reasonable expenses of administering the plan (exclusive benefit rule)
-  Carrying out duties with care, skill, prudence and diligence (prudent person rule)(*e.g.*, develop processes and procedures to demonstrate prudent decision making for ERISA plans such as Plan Investment Policy Statement, Benefits Committee meetings and Minutes, RFPs for service providers)
-  Diversifying plan investments to minimize risk of large losses (diversification rule)
-  Following plan document terms (unless inconsistent with ERISA), interpreting provisions, maintaining plan documents

Develop a Benefit Plan Cybersecurity Policy

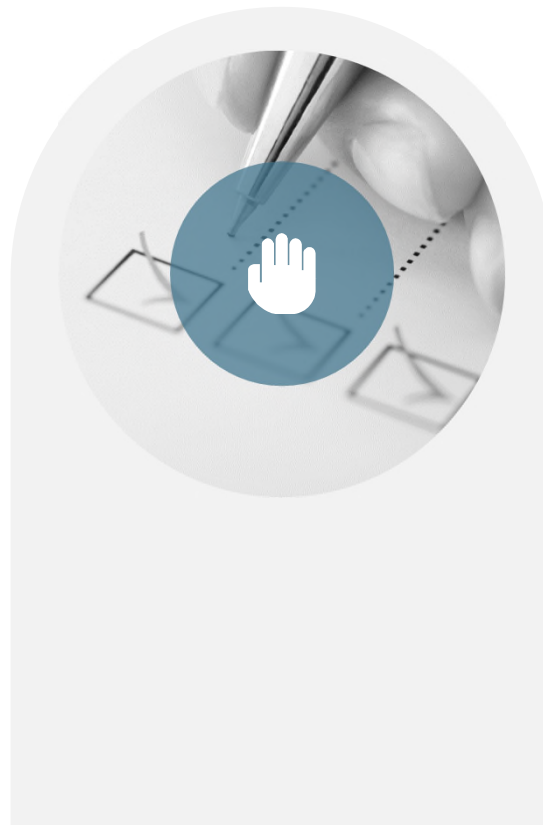
Establish the Approach

01 Assemble the Right Team

02 Identify the Data and the Risks

03 Train Employees

04 Develop Standards for Selecting and Monitoring Service Providers and Tools/Apps



05 Document Due Diligence

06 Address Data Privacy and Security in Service Agreements

07 Educate Participants

08 Cybersecurity Insurance

09 Adopt and Maintain the Benefit Plan Cybersecurity Policy

Develop a Benefit Plan Cybersecurity Policy

Assemble the Right Team

Consider

Existing organizational cybersecurity leaders

Benefit Plan Committee members

IT

Human Resources

Compliance

Risk Management

Legal

Outside Assistance

Develop a Benefit Plan Cybersecurity Policy

Identify the Data and the Risks



Personally Identifiable Information

All types of Information of Employees/Participants that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual such as:

- Names
- Addresses
- Date/Place of Birth
- Social Security Numbers
- Mother's Maiden Name
- Financial Information

Consider ways it is **Collected, Processed, Accessed, Transmitted, and Stored**



Protected Health Information

- Any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity (or their business associate), and can be linked to a specific individual
- Consider ways it is **Collected, Processed, Accessed, Transmitted, and Stored**

Develop a Benefit Plan Cybersecurity Policy

Train Employees

Hold employees who manage and have access to the data to the highest standards

01

02

Train employees on various scams (e.g., email, phishing)

03

04

Maintain lines of communication within the organization

05

Ensure adherence to security procedures (e.g., network protections, encryption processes, secure transmission and storage/destruction, limited access, password updates)

Develop a business response plan to deploy in the event of a data breach

Develop a Benefit Plan Cybersecurity Policy

Develop Standards for Selecting and Monitoring Service Providers and Technological Tools/Apps



- Confirm their cybersecurity program and certifications
- Review their Service Organization Controls
- Understand chains of delegation of work to agents, subcontractors, cloud vendors
- Determine procedures for data breach notification
- Examine protocols of tech tools and apps that will be provided to participants
- Discuss and develop reasonable procedures for data interactions (such as enhanced authentication measures for account access, distribution requests)
- Confirm levels of insurance including cybersecurity insurance
- Consider conducting a Risk Assessment
- Establish Procedures for Ongoing Monitoring

Develop a Benefit Plan Cybersecurity Policy

Document Due Diligence

Consider the following:

1

Incorporate data privacy and security questions into any requests for proposal and retain responses with plan records

2

Periodically review adherence to the security standards (*e.g.*, request updates, review reports, conduct audits, address review in plan Committee minutes)

3

Perform periodic risk assessments

4

Document any training sessions

Develop a Benefit Plan Cybersecurity Policy

Address Data Privacy and Security in Service Agreements

- Include representations and warranties regarding data privacy and security

- Include security audit provisions

- Confirm data breach notification policies and procedures and address in agreement

- Address insurance issues

- Address and/or consider impact of any limitation of liability or indemnification provisions especially in the event of a data breach

- Have agreement reviewed by IT, legal

Develop a Benefit Plan Cybersecurity Policy

Educate Participants

Consider educational tips to provide such as:

Remind employees regarding the importance of safeguarding their data at all time and warn against scams

Encourage use of passwords with a high level of security that are regularly updated

Advise participants to safeguard and monitor activity in their accounts

Remind employees to avoid posting too much personal information on social networking sites or reviewing sensitive data on public computers or kiosks

Develop a Benefit Plan Cybersecurity Policy

Adopt and Maintain the Benefit Plan Cybersecurity Policy

Adopt the Policy (consider incorporating into organizational policies as well as plan fiduciary best practice policies)

1

Conduct Periodic Reviews

2

Review updated audit reports

3

Implement Upgrades

4

Communicate with Service Providers

5

Undertake due diligence of new technology/apps

6

Update Service Agreements to include latest data privacy, security and data breach notification provisions and protections

7

EPSTEIN
BECKER
GREEN

Pay Equity Audits

Presented by



Nancy Gunzenhauser Popper

Associate – New York

npopper@ebglaw.com

212-351-3758



Alyssa Muñoz

Law Clerk – New York

amunoz@ebglaw.com

212-351-4757

Why Conduct a Pay Equity Audit?

Pay Equity Audits



Pay equity and Equal Pay Laws continue to be a hot topic

In response, several states and cities have amended or expanded their Equal Pay Laws

- California, Delaware, Maryland, Massachusetts, New Jersey, New York, and Oregon
- Revised definitions
- Pay Transparency provisions
- Salary History Inquiry bans



Voluntary self-evaluations may provide defense for employers

- Safe Harbor – unless you do nothing



Employee engagement



Objectives of Pay Equity Audits

What is the end result?



1. Identify whether pay inequity exists that cannot be explained by neutral, bona fide factors; and

2. Determine whether an employer's policies are creating or contributing to these inequities

Identify the Scope of the Audit

Starting Point and Factors to Consider

Opportunity to establish goals for the audit and get all parties on the same page

- Stakeholders
- Timing

Identify the departments, positions, location in scope

- Will vary depending on state and local Equal Pay laws
- Use caution when deploying targeted/narrow audits

It's an ongoing conversation

Establish and preserve attorney-client privilege and work product

Consider evaluating all employees' pay rates

Comparators

- Comparable work;
- Substantially similar skills, effort, and/or responsibilities;
- Geographic location;
- Similar working conditions

Sex/Gender; Other protected categories

- What type of Compensation do these populations receive?
 - Base compensation
 - Pay rate changes

Conducting the Audit

What Tools or Resources are Needed?



Data!

- Identify the system(s) where it is stored



Gather any data maintained on the demographics of the workforce

- Job grades/positions
- Salary ranges and tiers
- Employee demographic data – where are your women, minority, and older workers located in the organization?



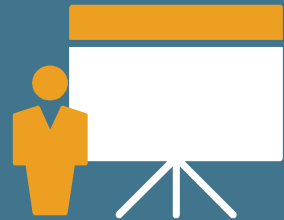
Gather current procedures and processes regarding compensation

- Base Compensation and Pay Increases
- Performance evaluations
- Job descriptions
- Training programs




Factors that managers use or rely on when making compensation decisions

- Don't have it easily accessible? Send questionnaires to your managers, ask them to submit descriptions of their process for determining pay changes.




Conducting the Audit

Dig into the Data... *Round 1*




Typically, pay equity audits will compare the average pay of men to the average pay of women, or individuals belonging to other protected categories to identify areas of concern.



Perform statistical analysis to determine if sex or any other protected category has an impact on pay rates.

- Separate the individuals that belong to the protected category from those that do not (e.g. men versus women)
- Examine data by looking purely at position and grade



Based on your review of Company processes and procedures, consider whether these have been applied consistently.

- Along with analysis of position and grade, begin tracking or note factors that will apply to the employees being reviewed

Conducting the Audit and Taking Remedial Actions

Dig Deeper into the Data... Round 2



Conduct a subsequent review of any specific employees and/or job positions where disparities exist.

- Additional errors or unexpected disparities may also surface

Assess whether the disparity is based on legitimate, neutral factors. For example:

- Length of service
- Education
- Geographic location
- Years of experience in the industry



Be fluid. Expect to move between the initial analysis and subsequent review more than once.

Taking Remedial Actions

Address Unjustified Disparities

Be prepared to address any disparities that cannot be identified as based on neutral, bona fide factors.

- Must increase the pay rate of affected employee(s) so that their pay rate is comparable to the work they are performing.
- Cannot adjust a higher paid employee down to the lower paid employee(s) rate.

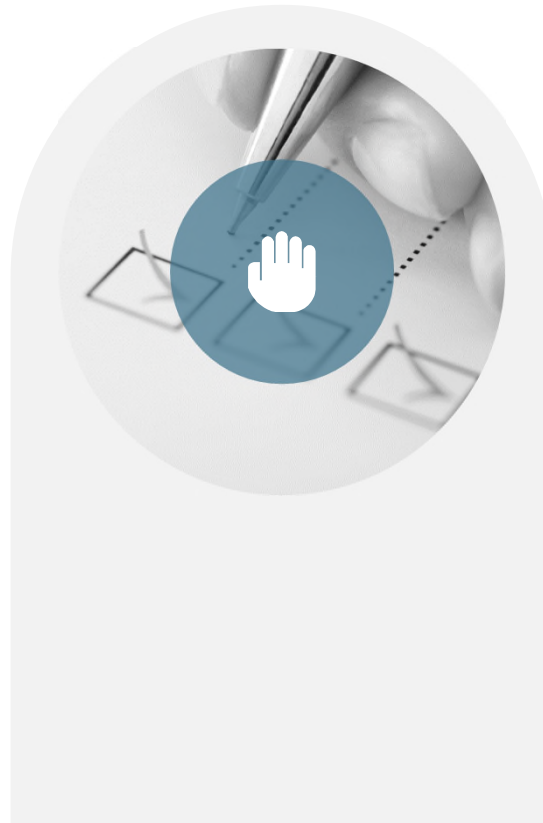
Use caution when making ad-hoc or off-cycle pay adjustments.

- Communicate effectively;
- Provide honest, but more general reasons for the pay adjustment;
- Maintain employee engagement and morale.

Best Practices Going Forward

What Should Employers do after a Pay Equity Audit?

- 01 Remain compliant with all laws, including Salary History Ban legislation.
- 02 Review and revise job descriptions and job grades, as needed.
- 03 Consider implementing standard pay ranges or guidelines for each grade/job classification.
- 04 Review and revise existing performance evaluations.



- 05 Review hiring practices
 - Applications
 - Recruitment process and procedures
 - Salary ranges
- 06 Train management, Human Resources staff, recruiters and compensation partners on applicable state and local laws.
- 07 If discrepancies appear, correct them!

Industry Spotlights Webinar Series: Big Data's Impact on Employers

May 30, 2018