Best Practices for ERISA Fiduciary Responsibilities and Cybersecurity for Retirement Plans

MICHELLE CAPEZZA AND CHRISTOPHER LECH, EPSTEIN BECKER & GREEN, P.C., WITH PRACTICAL LAW EMPLOYEE BENEFITS & EXECUTIVE COMPENSATION

Search the Resource ID numbers in blue on Westlaw for more.

A Practice Note providing for cybersecurity best practices for retirement plans to address fiduciaries responsibilities imposed by the Employee Retirement Income Security Act of 1974 (ERISA).

The Employee Retirement Income Security Act (ERISA) imposes specific duties and obligations on employers, individuals involved with retirement plans and other entities, including special rules applicable to those falling within the definition of a "fiduciary" in ERISA Section 3(21) (29 U.S.C. § 1002(21)).

Data and personally identifiable information (PII) have become increasingly more vulnerable to attack as it travels on employer and third-party systems. This has been partially due to the recent advancements in plan administration, technology, online enrollment and electronic access to account information, electronic delivery of disclosures including benefit statements, as well as benefit plan transaction processing (including self-certifications of distributions). In today's world, most transactions involving retirement plans are conducted electronically, including maintaining and sharing data and information across multiple platforms.

With the ongoing advancements in technology (including technological tools that have emerged to aid in the administration and delivery of employee benefits) and the novel cybersecurity risks that those advancements bring, there is widespread concern for both:

- The security of the employee data that is collected, transmitted, processed, and stored for employee benefit plans.
- The security of the assets in participant accounts.

To date, there are protocols and guidance for the privacy and security of protected health information (PHI) but there are no clear protocols for ERISA plan fiduciaries to ensure the security of PII, despite their equal vulnerability to data breaches.

Understanding ERISA fiduciary obligations to protect against employee benefit plan participant data breaches presents a challenge because of:

- Movement towards federal cybersecurity legislation is on the horizon.
- Varying state laws on privacy and data breach notification requirements.
- Scrutiny over financial institutions and their compliance with laws designed to protect PII.
- Increasing importance on HIPAA and HITECH compliance in the wake of health plan data breaches.
- Emerging litigation.

Fiduciaries are charged with meeting a prudence standard when discharging their duties solely in the interest of plan participants and beneficiaries and as applicable, must:

- Act prudently in responding to a breach of their plan participants' PHI and PII.
- Consider developing prudent policies and procedures for handling, collection, transmission, security and storage of all PII, data, and PHI.
- Consider developing third-party procedures and notification and remediation measures for breaches of their plan participants PHI and PII.

This Note provides guidance for plan fiduciaries of retirement plans to develop prudent policies and procedures to secure information and data. For a basic framework plan fiduciaries must consider for their responsibility to protect PII and data, see Practice Note, Cybersecurity and ERISA Fiduciary Responsibilities for Retirement Plans (W-024-1935).

ESTABLISH CYBERSECURITY POLICIES

Plan fiduciaries must always carry out their duties with prudent procedures and processes. Development of best practices related to cybersecurity requires thought and insight depending on the facts and circumstances.

© 2020 Thomson Reuters. All rights reserved.

Establishing an appropriate cybersecurity policy for retirement plans (Policy) is complicated because:

- This area is evolving and questions regarding ERISA preemption and conflicts with state and federal data privacy laws are not yet definitively addressed.
- Remediation of financial harm to a participant is difficult because the level of resulting financial injury may not be immediate or easily quantifiable.

When it comes to prudent selection and monitoring of plan service providers that intend to handle PII, due diligence of the third-party service provider's systems, data storage, and encryption security are all critical. Responsibilities to company personnel that handle the PII should also be prudently delegated.

Plan sponsors and fiduciaries should:

- Prepare and follow individualized Policies that suit their organization.
- Require third-party service providers to demonstrate compliance with Policies.

The Policy itself should reflect what is actually to be done and not include items that are not to be followed. This practice of developing and following a prudent Policy enables plan sponsors and fiduciaries to act prudently and mitigate their risk of breach of fiduciary duty claims by implementing best practices and following prudent policies and procedures to address cybersecurity of participant data.

In developing these Policies, consider the following:

- Assembling a team (see Assemble a Team).
- Identifying data (see Identify the Data).
- Data retention policies (see Data Retention Policy).
- Training employees handling data (see Train Employees Handling Data).
- Communicating with and educating employees (see Communicate with and Educate Employees).
- Remote working issues (see Remote Working Issues).
- Prudent standards for selecting an monitoring service providers (see Prudent Standards for Selecting and Monitoring Service Providers).
- Mobile app security (see Review Mobile App Security).
- Suggested RFP Questions from the 2016 ERISA Advisory Council (see Suggested RFP Questions from the 2016 ERISA Advisory Council).
- Service agreements (see Service Agreements).
- Cyberinsurance (see Cyberinsurance).
- ERISA bonding (see ERISA Bond).

ASSEMBLE A TEAM

Given the complexities involved in understanding data systems and security controls, organizations must assemble a qualified team of individuals to ask the right questions and review and interpret the answers.

The team may include individuals from:

- HR.
- IT.
- Legal.
- Compliance.
- Risk management.
- Any organizational cybersecurity leaders.

The team should identify its areas of risk and define its protocols around:

- Benefit plan data collection.
- Transmittal.
- Processing.
- Storage.
- Encryption.
- Outsourcing.
- Breach notification and response.

These developed protocols should then be properly executed and updated in compliance with applicable laws.

Designated employee benefit plan fiduciaries should incorporate organizational protocols in an approved Policy as part of its fiduciary best practices for benefit plan governance. To the extent the organization has an already developed data and information security program as an employer, it should be incorporated into benefit plan management practices. If an organization does not have adequate in-house resources to develop these data and security programs, it should obtain qualified outside assistance.

IDENTIFY THE DATA

The plan sponsor and fiduciaries should know what participant and beneficiary information and data is collected, transmitted, processed, and stored. PII and data typically at issue includes:

- Social Security numbers.
- Birth dates.
- Addresses.
- Beneficiary names.
- Addresses.
- Financial information.
- Account information.

Organizations must define the types of employee data that they are handling and set parameters regarding its maintenance and security. Employee benefit plans store extensive amounts of PII for participants and beneficiaries, which may be accessed by various personnel and service providers and makes it vulnerable to data breaches.

An initial step should focus on limiting the amount of information that is collected to categories that are absolutely crucial for the maintenance and administration of the plan. Depending on the type of benefit plan program, privacy and security may require vetting using different channels.

With a retirement investment advice tool, plan fiduciaries should undertake due diligence of the tool and the provider's privacy and security measures to protect PII.

Given the lack of uniform legal requirements in this area, plan sponsors and fiduciaries should:

© 2020 Thomson Reuters. All rights reserved.

- Be mindful of various state and local laws that may impact, among other things, the collection, storage, and transmittal of this PII.
- Understand the definition of PII can vary depending on the jurisdiction in which the plan is administered or the participant is located.
- Be cognizant of the types of data that is collected from participants and beneficiaries and the parties given access to it, the types of data that is shared with outside plan service providers, ways to limit the amounts of data shared, and methods to protect the security of the data in different environments.

An organization's general Information Security Program should already have identified data points and be in compliance with applicable laws. These should be followed for benefit plan purposes.

DATA RETENTION POLICY

Plan fiduciaries and sponsors should limit the amount of data that is collected to that which is absolutely necessary. A corollary to that step is the deletion of data that is no longer necessary or no longer required to be maintained by document retention laws.

Plan records generally must be retained for at least six years after the filing of a report (for example Form 5500 created from those plan records). For records necessary to determine a participant's or beneficiary's entitlement to plan benefits the records must be kept if a possibility exists that they may be relevant to a determination of the benefit entitlements of a participant or beneficiary. The latter requirement does not provide a clear timeframe for document retention.

Record retention policies must:

- Be designed prudently.
- Consider the various requirements and statutes of limitations.
- Be securely archived once a reasonable amount of time has elapsed, thus eliminating some of the risk associated with hosting that data on systems penetrable by hackers via the internet.

It is important to only keep data that is needed and use effective processes to discard unnecessary data, including back-up paper and electronic copies, and to reconcile procedure with applicable plan record retention requirements.

Electronic documents are not easily deleted and external service providers may also need to be consulted. For example, even when a document is dragged and dropped in the recycle-bin on a desktop, it may not be deleted off of the computer's hard drive or the cloud drive that is constantly backing up the data stored on the computer. Simply dragging and dropping a document into the recycle bin or hitting the delete button can leave meta data that contains an individual's personal email address, IP addresses, or other sensitive information contained within that document.

It is important to know where PII is located in all of the organization's systems and understand the security levels of any cloud computing and remote data storage processes that are involved in plan administration, including how data is stored or protected. In addition:

- Computer systems should be updated, including prompt installation of software patches.
- Electronic threats should be monitored in order to execute effective responses.
- Attention should be given to the National Institute of Security & Technology guidelines on computer configuration use.
- Attention should be given to full disk encryption on laptops and external data storage devices that might include PII or information on how to access it.
- The maintenance of a complete log-in for the network, firewalls, routers and key software applications should be implemented.
- The usage of portable devices and data storage devices that might include PII or information on how to access those devices should be limited or defined.

Where plan records are maintained by third-party service providers or recordkeepers, plan sponsors should ensure that service agreements address:

- Secure access to these records.
- Proper transfer, retention and destruction of records following termination of services.

Consultations with legal and IT departments and advisors can aid in determining:

- What information can be deleted.
- How information can be properly deleted.
- If information cannot be deleted but can be archived, how that information can be safely stored.

TRAIN EMPLOYEES HANDLING DATA

Organizations must:

- Ensure that all personnel given access to employee data are properly trained in safeguarding it, including securing the transmission of any data to third-party service providers.
- Ensure that internal personnel handling employee data are properly vetted.
- Ensure that proper measures are taken to protect against security breaches from within the company.
- Perform background checks on all individuals with access to PII.
- Ensure all personnel given access to PII are trained in properly safeguarding it. Include training in areas, such as data retention and destruction, social networking, social engineering, and litigation holds.
- Designate an individual to be in charge of privacy and security of PII.
- Implement and test contingency plans for use if a data breach occurs.
- Perform periodic risk assessments, maintain good controls, and be careful about which parties can override them.
- Train employees responsible for contract and vendor management regarding review of privacy and security issues in vendor arrangements.
- Ensure plan fiduciaries address how they intend to handle a data breach and response in the Policy.
- Designate and train individuals to respond to any benefits-related data breach and follow procedures for reporting breaches using the appropriate channels of the organization.
- Identify who must be notified at the company, what should be reported to any third-party service providers to coordinate remediation efforts, notification procedures and related tasks.

© 2020 Thomson Reuters. All rights reserved.

COMMUNICATE WITH AND EDUCATE EMPLOYEES

To communicate with and educate employees, organizations should:

- Inform employees about the importance of safe-guarding their data at all times.
- Warn against email and phishing scams.
- Encourage use of regularly updated passwords with a high level of security.
- Advise participants and beneficiaries to monitor their accounts.
- Focus on security measures in place for plan distributions, loans, and withdrawals.
- Prepare communications that remind participants and beneficiaries to safeguard their own benefit information, account balances, health information, passwords, and PINs.
- Advise against placing too much personal information on social networking sites and reviewing sensitive data on public computers or kiosks.
- Educate participants how to protect information by:
  - locking computers;
  - utilizing anti-spam and anti-virus tools;
  - hiding information from cameras;
  - setting up two-step authentication to access accounts;
  - shredding documents;
  - securely storing documents and addressing storage;
  - limiting sharing of devices;
  - being alert to phishing; and
  - protecting and updating passwords and PINs.

Determine whether to include specifics regarding these issues and the Policy in a plan document and summary plan description (SPD), so that it is clearly communicated and acknowledged by participants. Having clear language in a plan document and SPD regarding procedures participants must adhere to access their accounts and protect their data can serve as an extra layer of protection against fiduciary breach claims.

(See Summary Plan Description (SPD) Toolkit (3-519-2530).)

Plan sponsors should also consider the viability of including arbitration provisions within their plan documents and to the extent these arbitration provisions incorporate claims brought for cybersecurity breaches or mishaps. In Dorman v. Charles Schwab Corp., the Ninth Circuit overturned precedent and held that ERISA claims can be subject to mandatory individual arbitration and in a companion case, 780 Fed. App'x 510 (9th Cir. Aug. 20, 2019), upheld the plan's arbitration provisions and class action waivers (934 F.3d 1107 (9th Cir. Aug. 20, 2019)). Although questions remain, a plan provision requiring arbitration may include an ERISA Section 502(a)(2) claim brought on behalf of a plan, and class-waiver language may also serve to limit the scope of a dispute to losses to an individual account. It remains to be seen whether these types of provisions are likely to proliferate and whether they may be beneficial or burdensome if a cybersecurity breach case arises.

(See Arbitration of Disputes for Retirement Plans Toolkit (W-024-1898).)

Plan sponsors and fiduciaries should also determine whether any special notices or disclosures under state or other applicable law regarding the collection or use of participant data are required (for example, under the California Consumer Privacy Act), especially if ERISA preemption has not been reconciled.

REMOTE WORKING ISSUES

Working-from-home creates additional risk that employees may take shortcuts to ease working on personal devices or outside of the organization's regular environment. For example, employees may:

- Send emails or other documents that contain PHI or other personally identifiable information to their personal email addresses, which then may be automatically uploaded to their cloud-storage accounts.
- Upload sensitive data to their personal electronic devices that are unsecured or otherwise poorly protected.
- Physically take sensitive information home, either printed in hard copy or on flash drives, which can be lost or negligently shown to other individuals also working from home.

Similarly, hackers seeking to exploit the chaos surrounding COVID-19 can send out phishing emails purporting to provide vital company policy or coronavirus updates, through which they request personal or essential login information, in turn providing the hackers with the opportunities to infiltrate the organization's networks and databases.

It is impossible to predict or protect against every type of cyberattack, but plan sponsors and fiduciaries can take special actions to educate remote workers to protect sensitive data related to benefit plans:

- Send out reminders to employees to be extra vigilant in these times.
- Provide access to cybersecurity training or webinars so that employees are reminded how to identify various phishing scams and similar online attacks.
- Continuing ongoing communication efforts as outline above.

PRUDENT STANDARDS FOR SELECTING AND MONITORING SERVICE PROVIDERS

Plan fiduciaries should:

- Establish cybersecurity guidelines for engaging, monitoring, and renewing service providers, such as confirmation of their cybersecurity program and certifications, details regarding how they encrypt and protect data, their breach notification procedures, and a review of their Service Organization Control Reports or similar reports regarding their privacy and security controls, levels of insurance, and scope of their assumption of liabilities.
- Request information regarding the service providers' processes and systems for addressing cybersecurity threats and protection of PII, as well as past data breaches.
- Ensure third-party provider subcontractors are held to same standards as the service provider.
- Develop a record of diligence efforts undertaken to document the level of security of third-party service providers.
- Understand where data is stored and how it is secured and protected.

© 2020 Thomson Reuters. All rights reserved.

- Engage expertise of company IT professionals and legal counsel to review service agreements and provisions regarding data security, data storage, websites, breach notification, and confidentiality and develop parameters for compliance representations and indemnification in service agreements.
- Establish procedures for any IT security review of service provider systems, including requests for penetration tests to detect security risks, and identify those able to speak with vendors (for example, IT professional to IT professional).
- Develop a list of due diligence questions to ask service providers in connection with RFPs and contract renewals and select those providers with demonstrated security programs.
- Understand whether the service provider utilizes agents or subcontractors to perform the services and the chain of security measures and indemnification.
- Understand how data is accessed by participants and third parties, such as through online access or requests for retirement account distributions or transfers.
- Request that the service provider use enhanced measures, such as two-step or even three-step authentication, for participants to access the information (if not already doing so).
- Consider having the service providers generate and issue more complex usernames and passwords, as participants frequently use the same passwords and usernames across different websites.
- Consider setting up alerts for unusual behavior and educate employees on the steps they can take to protect their benefit plan information.
- Communicate with service providers as partners in the effort to protect plan data. Maintain open lines of communication and report suspicious activity.
- Connect organizational IT professionals with service provider IT professionals to address issues.

(See Practice Note, Negotiating ERISA Service Provider Agreements (4-616-5158) and Choosing Retirement Plan Service Providers Checklist (8-616-8348).)

REVIEW MOBILE APP SECURITY

The security of mobile apps should be reviewed as many new mobile apps allow plan participants to:

- Check account balances, contributions, and investment changes.
- Request loans or distributions.
- Receive alerts and educational information.
- Track financial and physical wellness and collect and convey this information to benefit plans.

Despite their convenience, the use of mobile apps provides yet another opportunity for data breaches or the actual theft of assets and benefit payments. Plan fiduciaries should ensure that the Policy sets out the protocols that should be followed when introducing apps into any benefits program.

SUGGESTED RFP QUESTIONS FROM THE 2016 ERISA ADVISORY COUNCIL

When contracting with service providers for plan administration, the service providers are given access to plan data, which may be a potential source of a breach. The most optimal time to address cybersecurity with a service provider is in an RFP stage. The 2016 Council suggested the following questions regarding the protection of data which may be helpful when contracting with and evaluating service providers:

- Does the service provider have a comprehensive and understandable cybersecurity program?
- What are the elements of the service provider's cybersecurity program?
- How is plan data to be maintained and protected?
- Is the data to be encrypted at rest, in transit, and on devices and is the encryption automated (rather than manual)?
- Is the service provider assuming liability for breaches?
- Is the service provider stipulating to permitted uses and restrictions on data use?
- What are the service provider's protocols for notifying plan management in the case of a breach and are the protocols satisfactory?
- Has the service provider agreed to provide regular reports and monitoring and what are they to include?
- Does the service provider regularly submit to voluntary external reviews of their controls (such as System and Organization Controls (SOC) reports or a similar report or certification)?
- What is the level and type of insurance coverage that is available?
- What is the level of financial and fraud coverage that protects participants from financial damage?
- If the service provider subcontracts to others, is the service provider insisting on protections in its agreement with the subcontractor?
- What controls does the service provider have in place over physical assets that store sensitive data, including when these assets are retired or replaced (for example, servers, hard drives, mobile devices)?
- What are the service provider's hiring and training practices (for example, background checks and screening practices and cyber training of personnel)?

SERVICE AGREEMENTS

Under the standards of the organization's Policy, the following should be addressed in the service agreement:

- Data privacy and security.
- Breach notification procedures.
- Liability.
- Indemnification provisions.

Plan fiduciaries should also:

- Request periodic updates from their service providers on the cybersecurity measures they follow and any new initiatives which should be further noted in meeting minutes.
- Ensure an emergency response game-plan is in place that meets standards under applicable law to communicate any data security breach to participants, beneficiaries, and appropriate authorities.
- Engage in due diligence for any service tools or apps (some apps may have a combination of financial, retirement plan and health

© 2020 Thomson Reuters. All rights reserved.

plan tools which may require review under a broader array of privacy laws, HIPAA, and state law requirements).

- Review and negotiate service agreements at the same level of detail as other service provider agreements.

Provisions to consider for a service agreement may include:

- **Data privacy addendum**. Benefit plan service provider service agreements should include provisions addressing cybersecurity for benefit plans, including any breach notification and remediation procedures. It is common to request that the agreement include a Data Privacy Addendum which may be offered by the service provider to reflect their information security program or a plan sponsor may have their own form which needs to be reviewed and negotiated for inclusion in the agreement. The Data Privacy Addendum should:
  - identify and define in the agreement (or appropriate exhibits incorporated by reference) the security protocols that are to be used with for plan transactions and distribution requests (for example, encryption, two-step authentication); and
  - address compliance with applicable privacy and security laws and industry standards.
- **Indemnification**. These provisions should be reviewed and negotiated to contractually address risk and extent to which it is to be redirected to third parties.
- **Limitation of Liability**. Ascertain whether the limitations of liability can carve out caps as they may apply to cybersecurity breaches. At a minimum, negotiate away caps on costs for breach notification and remediation costs.
- **Use of data**. Define any limitations that should apply on use of participant data (for example, use solely for intended services under the agreement, location of processing and storage, applicable data transfer restrictions). Define applicable law for offshore data storage (for example, follow US law to maintain data under applicable states requirements regardless of where data is managed, unless a more stringent law applies).
- **Breach response plan**. Define how the event of any breach is to be handled (for example, define breach remediation and notification procedures and timeline and which party pays costs). Negotiate right to review breach communications before they are distributed to participants.
- **Right to audit and security program updates**. Establish parameters for auditing third-party systems, receiving SOC reports, receiving security program updates, and rights to make any related requests based on any audit or review.
- **Customer guarantees**. If a service provider offers a customer guarantee, it is prudent to specifically incorporate it into the service agreement.
- **Agents and subcontractors**. Negotiate service agreement privacy and security terms that also apply to any service provider agents and subcontractors including destruction of data.
- **Termination of services**. Factor cybersecurity considerations and related provisions into scenarios when services may be terminated, especially with regard to transmission, storage and destruction of data.
- **Vendor insurance**. Confirm limits that apply to vendor's applicable cyber coverage, request certification of same, and define available coverage in service agreement.

CYBERINSURANCE

In addition to any insurance maintained by a plan sponsor, cybersecurity insurance has emerged in recent years and can offer various types of coverage, including coverage for certain disaster recovery and data breach response assistance that can be triggered by a benefit plan on a security breach. It is important for organizations to:

- Assess existing insurance and liability coverages to ascertain how cybersecurity insurance can fit within employee benefit plan insurance needs.
- Evaluate any cybersecurity insurance to ensure that it does not carve out and exclude the specific coverage that is desired and then make any appropriate adjustments.
- Determine any available coverage from a service provider and its interplay with the plan sponsor's own coverage.

In the Council's 2016 Report, it was noted that many insurance carriers now offer cyber insurance policies to augment existing insurance protection. In addition to third-party damage and defense costs, cyber insurance policies may include "first party coverage," which means that an insured does not have to wait for a third party to sue the plan. This type of coverage may:

- Apply to:
  - cyber extortion;
  - data recovery;
  - business interruption; or
  - bad actors preventing an organization from operating.
- Cover costs related to investigations and monitoring.

With this coverage, the plan can trigger coverage on a breach to obtain direct risk management and services, such as disaster recovery and response assistance. Third-party coverage is triggered by a lawsuit and may include:

- Forensic investigations.
- The cost of legal advice or specialists
- The settlement of lawsuits.
- The cost of remediation.
- Regulatory liability.
- Media liability.
- Credit monitoring.
- Credit freezes.

The Council's 2016 Report advised that when considering the role that insurance is to play in a cybersecurity risk management strategy, it is important to:

- Determine what is included and excluded from insurance policies already in place should there be a cyber breach.
- Consider how the coverage compares to the cyber risk assessment.

© 2020 Thomson Reuters. All rights reserved.

- If the coverage limits are acceptable.
- Confirm whether policy terms and conditions of coverage can be complied with.
- Consider the types of protection needed (for example, protection for participants against financial damage in the case of a breach, first party coverage to offer material assistance to respond to and recover from a breach, and coverage of the costs related to required breach notification and the penalties for failure to comply with breach notification laws).
- Understand whether it may be necessary to review multiple policies as they can vary among carriers, understand what is covered and the exclusions.

Plan sponsors and fiduciaries should also keep records of any breach investigations and steps taken to remedy the breach. It is necessary to review fiduciary liability insurance and consider potential interplay between cybersecurity insurance.

(See Practice Note, Insurance for ERISA Fiduciaries (2-517-5994).)

ERISA BOND

With certain exceptions, ERISA plan fiduciaries and every person handling plan funds or property must be bonded. A plan official is considered to handle funds whenever his or her duties or activities pose a risk that the funds or other property may be lost if fraud or dishonesty occurs on the part of the person, acting either alone or in collusion with others (such as duties related to the receipt, safekeeping, and disbursement of funds and relationships that involve access to funds or other property or decision-making powers regarding funds or property that can give rise to the risk of loss).

The question arises whether ERISA bonds can or should be obtained at levels that effectively protect against theft of plan assets by a plan fiduciary or person handling plan funds or property via a cyber-crime. The underlying terms of any ERISA bond must be reviewed closely for exclusions in this regard.

(See Practice Notes, ERISA Bonding Requirements (9-503-3454) and Insurance for ERISA Fiduciaries (2-517-5994).)

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **legalsolutions.com/practical-law**. For more information or to schedule training, call **1-800-733-2889** or e-mail **referenceattorneys@tr.com.**

07-20

© 2020 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (http://static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf) and Privacy Policy (https://a.next.westlaw.com/Privacy).