

Morgan Lewis

Is your business compliant when  
handling confidential client  
information?



Steven W. Stone  
Beth D. Kiesewetter  
Jon Gerty  
Etienne Drouard  
Carsten Horter  
Afzalah Sarwar

July 15, 2009

[www.morganlewis.com](http://www.morganlewis.com)

© 2009 Morgan, Lewis & Bockius LLP

# Today's Presenters



**Steven W. Stone**  
Washington, D.C.  
202.739.5453  
sstone@morganlewis.com



**Beth D. Kiesewetter**  
Washington, D.C.  
202.739.5127  
bkiesewetter@morganlewis.com



**Jon Gerty**  
London  
+44.020.3201.5583  
jgerty@morganlewis.com



**Etienne Drouard**  
Paris  
+33.1.53.30.4412  
edrouard@morganlewis.com



**Carsten Horter**  
New York/Frankfurt  
212.309.6199  
chorter@morganlewis.com



**Afzalah Sarwar**  
London  
+44.020.3201.5590  
asarwar@morganlewis.com

Is your business compliant when handling confidential client information?

**Morgan Lewis**

# Introduction

# Discussion Topics

- Introduction
- Overview of law and developments in the United States and Europe
- Disclosure of client information to overseas affiliates
- Disclosure of client information to overseas regulators and governmental authorities
- Disclosure of client information to third parties
- Expected systems and controls to prevent client information security breaches
- Sanctions for security breaches and remedial measures
- Questions & Answers

# Overview of law and developments in the USA and Europe

# Overview – USA 1

- Privacy and Data Security Regulation
  - Federal Privacy and Data Security Laws
    - *Gramm-Leach Bliley Act (“GLB Act”)*
      - Regulation S-P – Financial Privacy Rule
      - Regulation S-P – Safeguards Rule
      - Regulation S-P – Disposal Rule
    - *Fair Credit Reporting Act (“FCRA”), as amended by the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”)*
      - “Red Flags” Rules, Special Rules for Card Issuers, Address Discrepancy Rules
    - *USA PATRIOT Act of 2001*
      - Sections 314(a)/314(b) – Information Sharing Provisions
      - Section 356 – Suspicious Activity Reporting
  - State Privacy and Data Security Laws
    - *Notification to Clients of Data Breaches*
    - *Reasonable Policies and Procedures to Safeguard Personal Information*
    - *Minimum Standards for Disposal of Records Containing Personal Information*
    - *Representations Regarding Privacy in Service Provider Agreements*

# Overview – USA 2

- GLB Act
  - Regulation S-P – Financial Privacy Rule
    - *Directs how customers' personal financial information may be collected and disclosed by financial institutions; enforced by Securities and Exchange Commission (SEC)*
    - *Financial institutions must provide privacy notices that explain how their non-public personal information (NPPI) will be used to:*
      - “Customers” at the time the customer relationship is formed and annually thereafter
      - “Consumers” if their NPPI will be shared with non-affiliated third parties
    - *Financial institutions must provide a method to opt-out of NPPI sharing with unaffiliated third parties*
  - Regulation S-P – Safeguards Rule
    - *Directs financial institutions to implement procedures to protect customer information from unauthorized use; enforced by SEC*
    - *Financial institutions must adopt written policies and procedures for administrative, technical, and physical safeguards to:*
      - Ensure the security and confidentiality of customer records and information
      - Protect against any anticipated threats or hazards to the security or integrity of customer records and information
      - Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer

# Overview – USA 3

- GLB Act (*continued*)
  - Regulation S-P – Disposal Rule
    - *Requires financial institutions using consumer report information to take “reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal”*
- FCRA Act
  - “Red Flags” Rules
    - *Financial Institutions must develop and implement a written Board approved Identity Theft Prevention Program that is designed to detect, prevent and mitigate identity theft in connection “covered accounts”*
      - What should be included in my “Identity Theft Prevention Program?”
      - What are “Red Flags?”
      - What is a “covered account?”
      - How do the Red Flags Rules impact my Service Provider relationships?
  - Special Rules for Credit and Debit Card Issuers
    - *Financial Institutions that issue credit or debit cards must establish and implement reasonable policies and procedures to validate an address change upon receipt of a request for an additional or replacement card that is received shortly after a notification of change of address for the same account*

# Overview – USA 4

- FCRA Act (*continued*)
  - Address Discrepancy Rules
    - *Financial Institutions that use consumer reports (including credit reports) must develop and implement reasonable policies and procedures designed to enable the financial institution to:*
      - Form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when it receives a notice of address discrepancy
      - Furnish confirmed address of consumer to the Consumer Reporting Agency in certain circumstances
- USA PATRIOT Act of 2001
  - Section 314(a) – Information Sharing with Regulators
  - Section 314(b) – Information Sharing with Third Parties
  - Section 356 – Suspicious Activity Reporting

# Overview – USA 5

- State Privacy and Data Security Laws
  - Overview of State Requirements
    - *Notification to Clients of Data Breaches*
    - *Reasonable Policies and Procedures to Safeguard Personal Information*
    - *Minimum Standards for Disposal of Records Containing Personal Information*
    - *Representations Regarding Privacy in Service Provider Agreements*
  - Massachusetts Requirement for “Written Information Security Program”
    - *Requires: (1) Designation of Person to Oversee Program; (2) Identifying and Assessing Internal and External Risks to the Security and Integrity of Personal Information and Evaluating and Improving Safeguards; (3) Developing Security Policies for Employees that Telecommute; (4) Imposing Disciplinary Measures for Violations of the Security Program; (5) Preventing Terminated Employees from Accessing Personal Information; (6) Verifying Service Providers are Capable of Safeguarding Personal Information and Contractually Requiring them to Maintain Safeguards; (7) Collecting the Minimum Amount of Personal Information Necessary; (8) Inventorying Records, Computer Systems and Storage Media to Identify Records with Personal Information; (9) Monitoring and Auditing Employee Access to Personal Information; (10) Reviewing the Program Annually or Whenever there is a Change of Business Practices regarding Protection of Personal Information; and (11) Documenting Responses to Security Breaches, Establishing Mandatory Post-Incident Review and Making Changes as Necessary to the Program*
    - *Also Requires any Person that Electronically Stores or Transmits Personal Information to Establish and Maintain a Security Program for its Computers and Wireless Systems that includes, among other things Authentication Protocols, Secure Access Control Measures, Encryption of all Transmitted Files*

# Overview - Europe 1

- EC Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (95/46/EEC) (the “Directive”)
  - UK Data Protection Act 1998
  - French Data Privacy Act no. 78-17 dated January 6, 1978, amended by the Act no. 2004-801 dated August 6, 2004
  - Implemented 2001 into the German Federal Data Protection Act enacted in 1978
- Directive on privacy and electronic communications (2002/58/EC)

# Overview - Europe 2

- The Directive:
  - Harmonises the data protection laws in EU Member States
  - Defines the concepts: personal data, data controller, data processor, etc
  - Sets out the rights of individuals: to be informed, to object, to consent, to have access, to request deletion of data
  - Regulates the transfer of data to non-EEA countries
  - Regulates online direct marketing (opt-in/opt-out)

# Overview - Europe 3

- Which European Member State's rules apply when transferring data?
  - Location of the data controller
  - Location of processing equipment in EU
- Common themes in the Directive:
  - Data Protection Principles
  - Individual consent
  - Exemptions

# Overview – Europe 4

## United Kingdom

- Data Protection Act 1998
  - Principles-based legislation
  - Eight data protection principles
  - Schedule 2 and 3 Conditions
  - Consent
  - Exemptions

# Overview – Europe 5

## Germany

- Amended Federal Data Protection Act implementing the Directive
- Principle: processing of personal data is prohibited without the consent of the data subject unless expressly permitted by law
- New law on governmental voluntary data protection audit
- Regulatory requirements for certain industries
  - E.g. financial institutions and insurance companies

# Overview – Europe 6

## France

- 1978: data protection law
- 1984: banking secrecy, as part of professional secrecy
- 1991: secrecy of correspondence
- 1993: data protection principles in the Labor Code:
  - information of employees on the nature and purpose of the data processing, consultation of the works council
  - no “consent” is required but a proportionality principle applies
- 2001: case law on employee email protection
- 2004: implementation of the Directive
- 2005: case law on employee file protection
- 2008: application of the blocking statute of 1980

# Overview – Europe 7

## France Cont'd

- Compliance with prior information principle of employees (Labor Code)
- Protection of Mail Secret (private use of e-mails)
- Protection of professional secrets in banking/insurance sectors
- Blocking statute

# Disclosure to overseas affiliates

# Hypothetical

The European subsidiary of a US brokerage company wishes to transfer data to the US parent company. What should it do?

# Overseas Affiliates - USA

- Regulation S-P allows the disclosure of non-public personal information to affiliated third parties
  - Consider accuracy of disclosures in Privacy Notices distributed to clients as well as Privacy Notices posted to relevant websites
- USA PATRIOT Act, Section 314(b), limits the entities with which information regarding customer identification and suspicious activities may be shared
  - Safe Harbor may permit sharing of customer information and suspicious activity information between the European subsidiary and the US Parent
- Consider the application of the US Parent's Identity Theft Prevention Program and Comprehensive Information Security Program to the transfer of Personal Information
  - Necessary contractual provisions regarding detecting, preventing and mitigating identity theft
  - Necessary contractual provisions regarding information security protocols
  - Cooperation agreements in the event of unauthorized access during transfer

# Overseas Affiliates – Europe 1

## General principle regarding Transfer of Data outside the European Union

*“...the transfer to a third country of personal data ... may take place only if ... the third country in question ensures an adequate level of protection”*

# Overseas Affiliates – Europe 2

## Solutions to general prohibition on transfer

- Consent of data subjects
  - Informed Consent, freely given and revocable on individual basis
  - Practical only for specific occasions, not for data bases
- Transfer necessary for the performance of an agreement
  - Only if “necessary for” and not “useful for” other purposes
- Safe Harbor Principles (Transfer to the US)
  - Subject to the DoC registration/control; annual audits
  - Not applicable to financial institutions; only for transfer to the US

# Overseas Affiliates – Europe 3

## Solutions to general prohibition on transfer

- Standard EU data transfer agreement
  - Standard clauses available at the [EU Commission Website](#)
  - Subject to the law of the data exporter in the EU
  - Grants data subject enforcement rights
- Group-wide Binding Corporate Rules (BCR)
  - Applies to all affiliates
  - Guidelines by the European Commission
  - No clear procedures for approval by Member States

# Disclosure to overseas regulators

# Hypothetical

The European subsidiary of a US-based bank is required to disclose information to the SEC as part of an SEC led investigation into alleged bribery offences under the Foreign Corrupt Practices Act 1977 not involving the bank.

What should the bank do?

# Overseas regulators - USA

- Regulation S-P allows the disclosure of non-public personal information at the request of governmental request or judicial process
  - Consider accuracy of disclosures in Privacy Notices distributed to clients as well as Privacy Notices posted to relevant websites
  - Consider requesting that all requests for non-public personal information be provided in writing
- USA PATRIOT Act, Section 314(a), requires financial institutions to provide information to governmental authorities regarding customers pursuant to certain types of requests which may not apply in this situation
- USA PATRIOT Act, Section 356, limits the information regarding suspicious activities and the filing and content of Suspicious Activity Reports
  - Consider notifying FinCEN of the request
- Consider the application of the US Parent's Identity Theft Prevention Program and Comprehensive Information Security Program to the transfer of Personal Information
  - Consider safeguards that can be implemented in the transfer of the data
  - Consider encryption of nonpublic personal information
  - Consider requesting immediate notification in the event of unauthorized access during transfer

# Overseas regulators - Europe 1

- Compliance with Laws
  - US investigation in Europe is subject to local laws (data protection laws, criminal laws, regulatory laws)
- Possible Solutions
  - Transfer of personal data to the US: standard clauses, BCRs and Safe Harbour Exemptions will generally be impractical
  - Individual consent/anonymization where possible
  - Exception in the Directive: the transfer is permitted if “necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims”
  - Balance of Interest

# Overseas regulators – Europe 2

- Practical Advice
  - Know your obligations: internal due diligence on legal requirements in the EU
  - Communicate obligations to US courts and authorities: raising awareness
  - Negotiate and cooperate with US courts and authorities
- Preventive Measures
  - Establish Compliance and eDiscovery Guidelines

# Disclosure to overseas third parties

# Hypothetical

A US broker dealer wishes to sell the retail business of its European broker/dealer subsidiary to an unaffiliated buyer in the US. It is expected that client information of the European broker/dealer will be transferred to the buyer as part of the due diligence exercise and that the European broker/dealer's client accounts will be transferred following the sale.

What data protection considerations apply?

# Overseas third parties - USA

- Regulation S-P limits the disclosure of non-public personal information to unaffiliated third parties
  - Safe Harbor may permit sharing of non-public personal information to an unaffiliated third party in the event that such sharing of information is necessary for the performance of an existing agreement with the customer
    - *Considerations During the Due Diligence Process Include:*
      - Allowing a mutually agreed upon agent of each of the broker-dealers, such as an attorney or consultant, to perform the due diligence regarding customer account information prior to the execution of the Purchase and Sale Agreement and assignment of the customer brokerage agreements.
      - This service provider arrangement would require contractual obligations for the attorney or consultant such as that it has reasonable policies and procedures to detect, prevent and mitigate identity theft, it will not disclose the information to any other party, except with respect to the adequacy of due diligence, and it will adhere to the information security protocols (i.e., access controls, encryption) for such information sharing arrangements
      - Reviewing customer brokerage agreements to determine if any anti-assignment provisions would require customer notification and the execution of new brokerage account agreements
    - *Considerations Relating to the Closing Include:*
      - Consider non-disclosure and information security provisions in Purchase and Sale Agreement
- USA PATRIOT Act, Section 314(b), limits the entities with which information regarding customer identification and suspicious activities may be shared
  - Safe Harbor may permit sharing of customer information and suspicious activity information between the US parent and its European subsidiary and, in turn, information sharing between the US seller and US buyer

# Overseas third parties - Europe 1

- Examples of situations where processing of personal data applies
- Different considerations may apply depending if asset sale or share sale
- May need to notify clients whose data will be transferred
- Ensure that a legitimate ground exists for disclosure/processing by the parties
- Ensure adequate security measures are in place (e.g. data rooms)
- Ensure that appropriate mechanisms in place to lawfully transfer overseas

# Overseas third parties - Europe 2

- Consider amending data protection details with the relevant regulator
- Other considerations such as client money and issue of consent
- Other circumstances where data may be transferred to overseas third parties:
  - Sharing of information between lenders/credit reference agencies
  - Outsourcing (e.g. AML, complaints handling or invoice processing services)
  - Disclosing data to forensic agencies

# Expected Systems and Controls

# Expected Systems and Controls – USA 1

- Privacy Policies and Procedures
  - Provide customers with notice of the firm’s privacy policy and the opportunity to opt out from / opt in to having their information shared with non-affiliated third parties
  - Adopt written policies and procedures for administrative, technical and physical safeguards to protect customer records and personal information and for the appropriate disposal of records including personal information
- Identity Theft Prevention Program
  - Designate in writing a senior management committee or senior manager with responsibility for establishing and maintaining the program
  - Adopt written policies and procedures to address the Red Flag Rules that require financial institutions with covered accounts to detect, prevent and mitigate the identity theft, including:
    - *The identification of red flags or activities that may indicate the potential for identity theft*
    - *The detection of red flags that have been incorporated into the Program*
    - *Protocols for responding to red flags that are detected, which may include: (1) monitoring account activity, (2) contacting the customer, (3) checking similar accounts; (4) collecting and documenting security breach information (5) reporting unauthorized access to appropriate federal, state and self-regulatory organization authorities / SAR filing, (6) providing affected customers prompt notification consistent with federal and state requirements, and (7) providing affected customers assistance with how to mitigate the potential for identity theft*
  - Adopt written policies and procedures to address the Special Rules for credit and debit card issuers, to the extent applicable
  - Adopt written policies and procedures to address the Address Discrepancy Rules for users of consumer report information provided by Consumer Reporting Agencies, to the extent applicable
  - Train staff to implement the Identity Theft Prevention Program
  - Supervise service providers to determine that they have in place an Identity Theft Prevention Program and will alert you promptly if they identify red flags in connection with “covered accounts”
  - Evaluate and adjust the Identity Theft Prevention Program to reflect changes to regulations or business operations

# Expected Systems and Controls – USA 2

- Comprehensive Information Security Program
  - Designate in writing an employee or employees to coordinate the program
  - Adopt written policies and procedures
  - Identify in writing reasonably foreseeable security risks that could result in unauthorized disclosure, misuse, alteration, destruction or other compromise of *personal information or personal information systems*
  - Design, document and implement information safeguards to control identified risks
  - Regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems and procedures, including:
    - *Effectiveness of access controls on personal information systems*
    - *Controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons*
    - *Employee training and supervision*
  - Train staff to implement the information security program
  - Oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards
  - Evaluate and adjust information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the firm knows or reasonably believes may have a material impact on the program

# Expected Systems and Controls – Europe 1

- The Directive provides for :
  - Confidentiality of the processing,
  - Duty of Security (appropriate technical and organizational measures against accidental or unlawful manipulations)
  - All subject to the nature of the processing
    - *The level of security takes into account*
      - *the state of the art*
      - *the costs of their implementation*
      - *the risks inherent in the processing*
      - *the nature of the data to be protected*

# Expected Systems and Controls – Europe 2

- Security undertakings depend on
  - The nature of the data
    - *Covered by banking secrecy?*
    - *Accounting, customer, employee or IT data?*
    - *Are customers natural or legal persons?*
  - The authorized third-parties
    - *As designated by local laws or court-order*
    - *In compliance with the blocking statute if applicable*
  - The original purpose of the processing

# Expected Systems and Controls – Europe 3

- Safeguards
  - Restrict physical and logical access to IT systems and data
  - Provide for secure transfer
  - Control and track the input, change and deletion of data
  - Protect data from destruction, loss and unwanted alteration
  - Separate data for different purposes
  - Control contractors
- All subject to proportionality

# Sanctions and Remedies

# Sanctions & Remedies - USA

- Complaints from clients to regulatory authorities
- Investigation by regulatory authorities
- Enforcement action taken by SEC, FINRA, and/or state securities regulators
  - Censure / Fines / Disgorgement of Profits (if any)
  - Remediation / Independent Consultant Reviews
  - Public Disclosure Reporting Required
- Civil litigation

# Sanctions & Remedies – Europe 1

## United Kingdom

- Complaints from data subject
- Criminal offences
- Shortcomings of the UK sanctions
- Measures by the FSA
- Civil litigation

# Sanctions & Remedies – Europe 2

## Germany

- Different enforcement depending on federal or state
- Fines
- Public reproof by the authorities
- Establishment of remediation measures
- Criminal offences

# Sanctions & Remedies – Europe 3

## France

- Criminal Offences – up to 5 year of imprisonment and/or up to €300,000 (natural person) or €1.5m (legal person) in fines) for:
  - Non compliance with DPA's notification, security duty, data subject information or deceptive processing
  - Breach of privacy of mail or of professional secrecy
- Civil litigation
- Administrative proceedings (up to 300,000€ in fine)
- Public reproof by the CNIL or financial regulators
- Termination or the processing & deletion of the data/seizure of the hardware used for the processing

# Contact Information



**Steven W. Stone**  
Washington, D.C.  
202.739.5453  
sstone@morganlewis.com



**Beth D. Kiesewetter**  
Washington, D.C.  
202.739.5127  
bkiesewetter@morganlewis.com



**Jon Gerty**  
London  
+44.020.3201.5583  
jgerty@morganlewis.com



**Etienne Drouard**  
Paris  
+33.1.53.30.4412  
edrouard@morganlewis.com



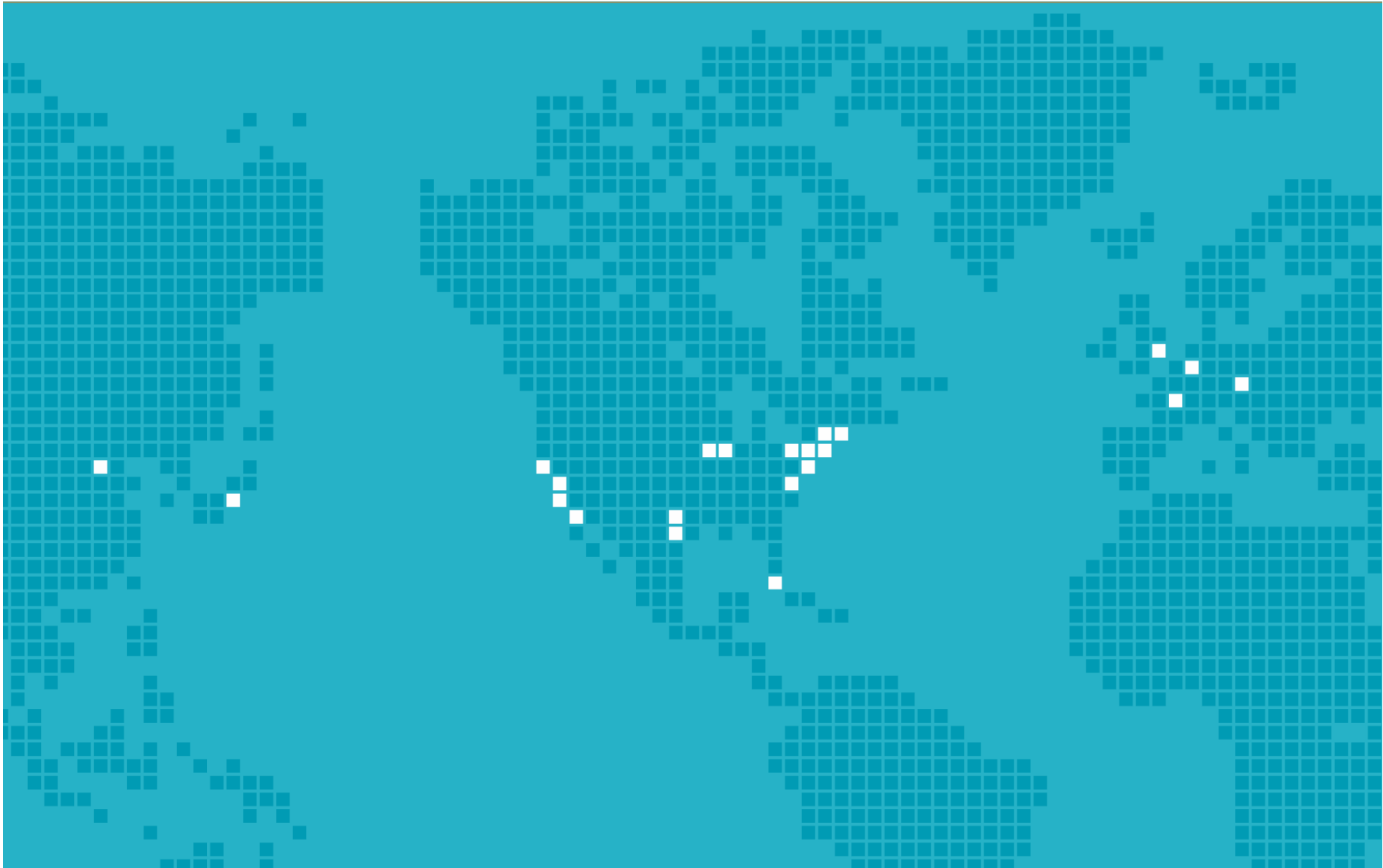
**Carsten Horter**  
New York/Frankfurt  
212.309.6199  
chorter@morganlewis.com



**Afzalah Sarwar**  
London  
+44.020.3201.5590  
asarwar@morganlewis.com

Is your business compliant when handling confidential client information?

# Questions and Answers



worldwide

Beijing Boston Brussels Chicago Dallas Frankfurt Harrisburg Houston  
Irvine London Los Angeles Miami Minneapolis New York Palo Alto Paris  
Philadelphia Pittsburgh Princeton San Francisco Tokyo Washington