



**Data privacy and corporate America:
who's recognizing the risk?**
April 2009



01
Contents

02 Executive summary

04 Introduction – recognizing the risk

06 Privacy and data security - the 10-K filing

07 The 10-K survey

10 Privacy and data security - who's encrypting?

11 The encryption survey

14 Time to recognize and manage the risk

16 Contact details

Statistics show that data breaches are becoming more frequent, more sophisticated and more financially damaging

In today's world, securing confidential information is no longer simply an information technology (IT) function but rather a business enabler. Entities handling the sensitive information of their customers or their clients' customers - including but not limited to health information, credit card information, or social security numbers - owe an ever increasing duty to protect that information. Yet, it is rare to meet someone who has not, in some way, been affected by a data breach; be it a call from their bank or credit card provider asking about an abnormal transaction, receiving a reissued credit card, or even free credit monitoring services. As news agencies report on an almost daily basis of yet another company suffering a security breach that has exposed the confidential information of customers, we are left to consider if companies are doing enough to prevent these events.

Statistics show that data breaches are becoming more frequent, more sophisticated, and more financially damaging. They show that the public and their governmental representatives are becoming more concerned with the threat of identity theft and have an expectation that companies are working diligently to protect the confidential information under their care, custody, and control.

Can we assume however that corporate America has a full appreciation for these exposures and expectations, and recognizes the potential financial and

reputational harm? Are US companies utilizing the best tools available to prevent a breach?

To help answer these questions, and in light of the increasing vulnerability of sensitive information and the resulting need for increased security and preparedness, this report:

- assesses the recognition companies give to privacy and data security by way of disclosure in their SEC 10-K filings
- discusses the benefits of encryption and reviews data regarding its use
- discusses the need for collaboration between risk management, IT and legal departments to identify and assess the obligations and benefits of data security best practices.

Key findings – 10-K Risk Factors

- 38 percent of Fortune 500 companies surveyed do not explicitly mention privacy/data breach in the Risk Factors section of their SEC 10-K filing. By industry breakdown this includes;
 - 46 percent of diversified financial companies
 - 40 percent of healthcare: medical facilities
 - 52 percent of specialty retailers
 - 50 percent of telecommunications firms
 - 80 percent of utilities firms.
- Of the companies that did include the risk of a data breach in their 10-K, 26 percent failed to mention the potential financial risk
- Just under half (49 percent) failed to identify the reputational risk.

Key findings – encryption

- Of the companies assessed in a separate study of 60 US organizations, only 7 percent had implemented end-to-end encryption of sensitive data
- 42 percent of the companies assessed had suffered a data breach, and of those only 12 percent had encryption in place for data at rest
- 47 percent of the companies assessed had not fully implemented laptop encryption
- 29 percent of the companies assessed had not fully implemented back-up tape encryption.

Conclusion

The evidence shows that companies do not yet appear to fully appreciate the exposure to their financial and reputational well-being that privacy and data security poses. They also do not appear to fully appreciate the benefits of the encryption of sensitive information, as well as its potential legal requirement.

The findings emphasize the need for, and benefits of, collaboration between the risk management, IT and legal departments to properly assess this exposure and the means by which it is addressed.

Access to one system could net a cyber criminal the confidential information of millions of individuals

We have been using computers and other technology for quite some time, but why does it seem that information security continues to lag behind? As our use of, and dependence on technology has continued to grow both at home and in the workplace creating an ever more connected society, so too has the focus by the criminal element on cyber-related crimes.

The infamous 20th century US bank robber Willie Sutton was once asked why he robbed banks, to which he responded, 'because that's where the money is'. Well today, the 'money' is stored on millions of computers throughout the world. And whereas you would need to rob multiple banks to obtain significant funds, data that can be used today to commit financial fraud is aggregated in massive quantities; access to one system could net a cyber criminal the confidential information of millions of individuals.

Legislating the risk

In recognition of this increasing exposure, governments and industry groups worldwide have established laws and standards for the protection of this data.

Beginning in 2003 with the California Senate Bill 1386, 44 US States and the District of Columbia currently have some form of data privacy law which requires

companies to notify individuals when their confidential information has been compromised.

In addition, the American Recovery and Reinvestment Act of 2009 which was recently signed into law, includes changes to the Health Insurance Portability and Accountability Act (HIPAA). Entities subject to HIPAA will now be required to notify individuals of a breach of unsecured personal health information that compromises the security or privacy of the information.¹ Although subject to change, the current standard for whether the data is secure is if it is rendered 'unusable, unreadable, or indecipherable to unauthorized individuals'. Could this change signal the beginning of more federal level notification laws?

Facing the fines

Mandatory disclosures, while they themselves can be costly, have now tagged the specific entity that has suffered the breach and have led to even more costly consequences. Federal commissions and regulatory bodies, state attorney generals, and specific industry groups have been compelled to take action on behalf of their constituents or members where they feel a company has not done all they should to prevent the breach, or was not compliant with the required standards.

The disclosures have in turn identified a class of individuals on whose behalf plaintiff attorneys have brought numerous actions. In the case of a disclosure of credit card data for example, numerous claims have been brought by banks and actions by the card companies themselves seeking reimbursement of the costs of any fraudulent charges, as well as to reissue cards.

Damaging reputations

A single breach or disclosure of confidential information, for example a lost laptop, can have far reaching consequences including reputational and financial harm. The costs of a single breach can mount very quickly; from the direct costs (notification of customers, providing credit monitoring services, defending and settling claims); to the indirect costs (lost employee productivity and the opportunity costs of lost customers and goodwill).

So what evidence do we have that US companies recognize the risk and understand the ramifications of a breach?

¹ www.hallrender.com

Only 62 percent mention privacy or data security exposures within the risk factors section of their 10-K filing

For public companies, one piece of potential evidence of this level of understanding and appreciation is in the publicly filed reports required by the US Securities and Exchange Commission (SEC).

On an annual basis, companies with more than US\$10 million in assets and whose securities are held by more than 500 owners, must file a 10-K report which provides a comprehensive summary of their performance. This includes a listing of Risk Factors, used to warn investors and potential investors of risks that could, if they occur, be expected to have a financial impact on the company.

The SEC has made clear what the required content is that must be included in the Risk Factors section of a 10-K filing. However, the flexibility that is afforded companies operating within certain industries invites interpretation and internal debate. One aspect open for interpretation focuses on privacy and data security issues.

The 10-K survey

Our research set out to identify those companies within the Fortune 500 who explicitly do or do not refer to the risk of privacy or data breach exposures within their 10-K filing Risk Factors section and, if they do mention the risk, whether they mention the potential reputational and/or financial impact of a breach.

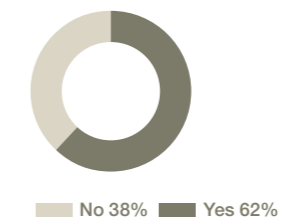
The research focused on the most recent 10-K filings, as of February 2009, of nearly

250 companies in those industry sectors within the Fortune 500 that would reasonably be expected to handle significant amounts of personal data; ranging from sectors such as airlines, banks, healthcare, leisure and utility companies.

The findings of the study were wide and varied. There are entities within sectors which have experienced large, financially significant data breaches and where you would expect a solid recognition of the exposure, that do not mention privacy or data security as a risk factor. Yet, other sectors were represented 100% in their recognition.

– Of the industry sectors reviewed, only 62 percent mention privacy or data security exposures within the Risk Factors section of their 10-K filing

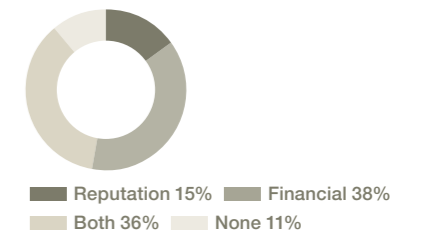
Percentage of Fortune 500 companies of select industries mentioning privacy/data breach risk in their 10-K



– Given that the study was focused on those select industries where data privacy and security would seem pertinent, 38 percent of companies not mentioning this as a risk factor appears to be a significant oversight

– Of those companies that did mention the risk of a privacy/data breach risk, 26 percent failed to mention the potential financial impact of a breach and nearly half (49 percent) failed to mention the potential impact on their reputation.

Mentioned impacts of privacy/data breach risk



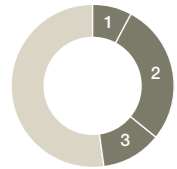
Analysis by sector

– By industry sector, one of the most attention grabbing results was the Specialty Retailer sector for which less than half (48 percent) of the companies mention privacy or data security in their Risk Factors section

– Only 40 percent of this sector discusses the potential financial impact of a breach. And only 28 percent publicize both the potential financial impact and the potential impact on the company's reputation

08
Privacy and data security
 the 10-K filing

Mentions of privacy/data breach risk and the potential impact for Fortune 500 Specialty Retailers

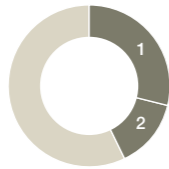


No 52% Yes 48%
 1. Reputation 8% 2. Both (financial & reputation) 28% 3. Financial 12%

Given that some of the largest and most highly publicized data breaches in history have been in the retail sector, including BJ's Wholesale Club, TJX and Hannaford, it is surprising to see any retail company not listing this as a risk factor.

- In the Life and Health Insurance sector, 57 percent made no mention of privacy or data security in their Risk Factors section
- Only 14 percent of these companies addressed the potential impact to their reputation

Mentions of privacy/data breach risk and the potential impact for Fortune 500 Life and Health Insurance Companies



No 57% Yes 43%
 1. Financial 29%
 2. Both (financial & reputation) 14%

- Given the amount of customer data they hold, it was a surprise that only 20 percent of companies in the Gas and Electric Utilities sector mention privacy or data security within their Risk Factors section

Mentions of privacy/data breach risk and the potential impact for Fortune 500 Gas and Electric Utilities Companies

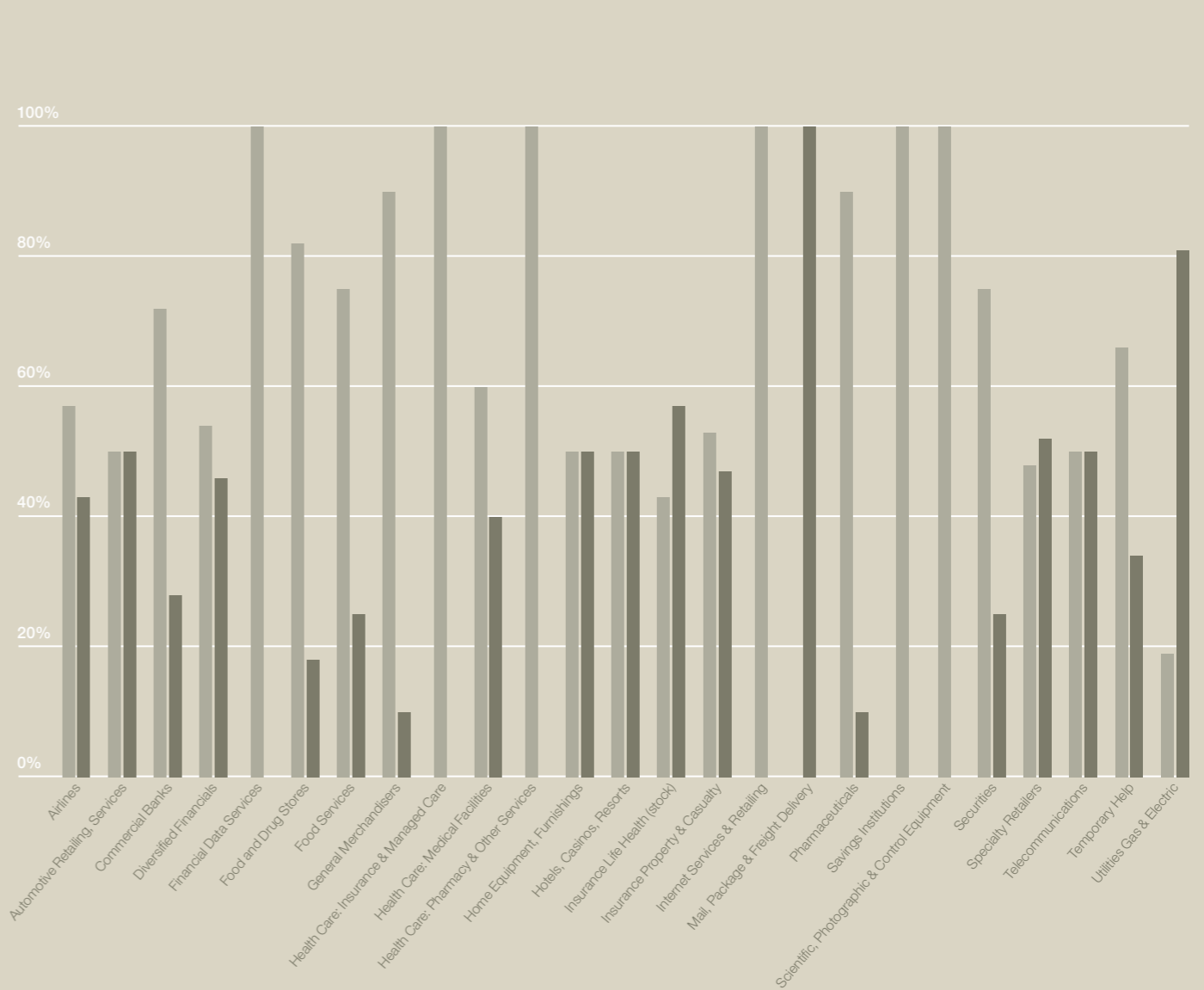


No 80% Yes 20%
 1. Financial 12%
 2. Both (financial & reputation) 8%

- Perhaps not surprisingly, all of the companies in the Internet Services and Retailing sector list privacy or data security as a risk factor. The perception is that these companies, from their inception, have understood the significance of their reliance on technology and data and have always had an appreciation for the inherent risks in their model. Yet still, 17 percent do not highlight the financial impact of a breach.

09
Privacy and data security
 the 10-K filing

Mentions of privacy/data breach risk in 10-Ks of Fortune 500 companies in selected sectors



Aside from whether a company has an appreciation for these risks, what steps then are they taking to prevent them?

To relate back to our earlier bank robber analogy, when cyber criminals 'steal' data, in reality they are often simply making a copy. So whereas at a bank it would be fairly obvious that the money is gone, that is not the case with data. Security at a bank is focused on physical attributes; a thick safe, limited knowledge of the combination, security guards, security cameras. While these elements are still important - you do not want someone walking into the computer server room and strolling out with the goods - there are significantly more layers required in the defense-in-depth approach to data security, including tightly controlled and monitored access.

Standards for information security have existed for some time now and in some cases they are mandatory; HIPAA (Health Insurance Portability and Accountability Act) for health care, GLBA (Gramm-Leach-Bliley Act) for financial institutions, and PCI/DSS (Payment Card Industry Data Security Standard) for those handling credit cards. As recent events have shown however, compliance with these standards does not mean there is no exposure.

Suffering a breach

In early 2009 Heartland Payment Systems, Inc. disclosed a breach that could prove to be the largest to date. After apparently weeks of tracking, Heartland, along with the US Secret Service and forensic experts, was finally able to locate malicious software that had been planted on their network. Robert

Baldwin, president and CFO of Heartland indicated that they did not know how long it had been there, how it got there, or how much data was compromised. According to CEO Robert Carr, Heartland processes about 100 million transactions a month.

The Heartland breach has once again prompted critics of the PCI/DSS. Heartland disclosed that a breach of its systems had compromised at least 4.2 million credit and debit card accounts, even though the company had reportedly been audited and deemed PCI/DSS compliant.

In a statement, Carr said, "There is no single silver bullet that will secure payment systems, and constant vigilance and monitoring of the infrastructure will always be required. Nevertheless, I believe the development and deployment of end-to-end encryption will provide us the ability to implement increasing levels of security protection as they become needed."²

Another line of defense

Encryption is not viewed as a stand alone solution but rather another layer in a defense-in-depth approach to security. It is another in the line of information security technologies, such as anti-virus software, firewalls, and intrusion detection systems, to be developed and adopted.

End-to-end encryption would encompass all elements of the network, including all points where the data resides at-rest, as well as in-transit on and exiting the network.

- Mobile computing devices (e.g. laptops)
- Storage devices (e.g. USB flash drives, CDs/DVDs, backup tapes)
- At-rest (e.g. databases, desktops)
- In-transit (e.g. intra-network, email, file transfers, remote access)
- Wireless access points

The most obvious beneficial implementation of encryption is when there is a risk of physical loss or theft of mobile computing devices such as a laptop or mobile storage devices such as USB flash drives or backup tapes. By implementing true end-to-end encryption, IT security can focus its attention on authorized access to the data and those instances when the data must be decrypted for use.

But are firms taking advantage of the benefits of encryption technology?

The encryption survey

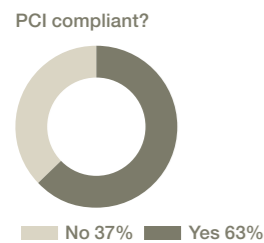
To assess the levels of encryption undertaken by corporate America, a snapshot picture of 60 organizations from sectors including healthcare, retail, and financial services; and ranging in size from those with revenues in the tens of millions to the largest companies with revenues in the billions, were surveyed jointly by Hiscox and cyber risk management assessment specialists NetDiligence® in 2008.

The results provided a remarkable insight into the lack of preparedness of many organizations when it comes to protecting themselves against a possible data breach.

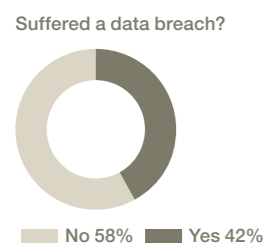
² <http://searchsecurity.techtarget.com.au>

12
Privacy and data security
 who's encrypting?

- 37 percent of those companies where PCI compliance is applicable were not fully compliant. This may be because many companies struggle with the approximately 230 specific control requirements that make up the standard which can be daunting and costly to achieve and maintain for any organization. PCI is also a 'living standard' in that the PCI Standard Organization tries to 'improve' their requirements and each year the standard changes (usually becoming more strict) making compliance more difficult



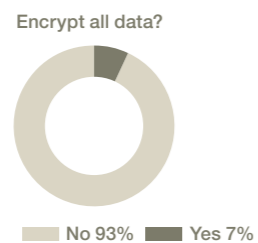
- Of those analyzed, 42 percent had suffered a data breach and 27 percent had to issue a notice of a data breach



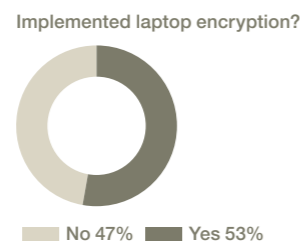
- Of the 42 percent who had suffered a data breach only 12 percent of those companies actually had encryption in place for data at rest

- With data held in a number of different forms (at rest, backup, in transit, email,

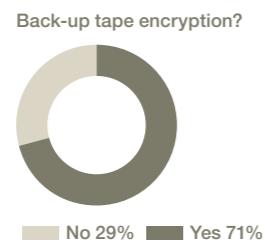
wireless, and laptops), and despite nearly half having suffered some form of a data breach, only 7 percent encrypted all their data in every form in which it is held.



- 47 percent of companies had not fully implemented laptop encryption



- 29 percent had not fully implemented back-up tape encryption



The benefits of encryption
 Encryption may not only reduce the incidence of data breaches occurring but can offer companies some degree of legal safe harbor if a breach was

to occur. Almost all of the 44 US state data privacy notification laws include some form of a safe harbor provision for encrypted data absolving the company of the obligation to notify in the event confidential data is compromised (for example, in the event of a lost or stolen laptop). These laws recognize that if lost or stolen data was encrypted, and did not include the encryption key, it is very unlikely that it will be misused. Although it would be less likely to be the subject of claims if there was no obligation to notify, encryption could still prove to be an excellent discouragement to legal action by third parties.

So why don't all companies encrypt their data?

The reasons are varied and range from cost, performance concerns, technical complexity issues, or simply a belief that encryption is overkill and other controls such as access controls, intrusion detection, and firewalls will be sufficient.

It should be noted however, that for some, encryption will be the only option. A new Massachusetts law scheduled to take effect in January 2010, requires any firm conducting business with state residents to deploy encryption and protect against data leakage. A combination of a person's name along with their Social Security number, bank account number or credit card number must be encrypted when stored on portable devices, or transmitted wirelessly on public networks, according to the new law.

13
Privacy and data security
 who's encrypting?

Only 7 percent encrypted all their data in every form in which it is held

Risk managers should work with their IT department to understand the degree to which the company handles sensitive data and how it's protected

In the 19th century, the adoption of fire protection in buildings was crucial for the continued and explosive growth of industry and urbanization. Today, the same risk management rigor must be applied to technology use as businesses face an explosion of data and the resulting challenges in its storage and maintenance.

As this report shows, companies do not appear to prioritize the data privacy and security risk. Traditional risks to the business such as that to property still take center stage when the potential damage of a data breach is just as significant as that of the factory burning down – and potentially more so due to the reputational aspects.

Insufficient standards

While many businesses have not been faced with a catastrophic breach, the recent incident at Heartland Payment Systems offers a major lesson: many of the standards for data privacy and security of data are not sufficient.

But as long as companies handle sensitive information; have a responsibility to maintain the privacy of that information; and are the target of cyber criminals; they will be subject to laws and regulations aimed at preventing a breach and will need or be required to seek solutions well beyond the standards.

Encryption should be a top priority for any firm handling material amounts of sensitive information as it provides safe harbors afforded by breach notification laws, adds benefits as a data protection tool, and will be required use by some pending laws.

Work together

The complexity of the data security landscape and the legal and regulatory environment highlights the need for legal, IT and risk management departments to work closely together to address the risks associated with data exposure. Risk managers should work with their IT department to understand the degree to which the company handles sensitive data and how it's protected. Risk managers and IT must also collaborate with attorneys and other specialists to understand their obligations and the ramifications of the various privacy and data security regulations. In an economic climate where IT budgets are tight, all should work together to analyze the cost/benefit of encryption relative to other projects.

The insurance view

Risk managers may also seek to transfer some of this risk via insurance. In light of the increasing exposure, regulatory scrutiny, legal obligations and resultant claims and losses, insurance providers will respond by having higher expectations regarding an applicant's understanding and response to the risk. This includes the encryption of sensitive data. And while insurance companies continue to move into this space, risk managers should be wary of any insurer that does not have high expectations regarding the applicant's best practices. A major lesson learned in the recent financial industry crisis is that companies willing to assume toxic risks in search of greater top line growth and return will not be stable, long term partners. In the insurance world, stability and long term claim paying ability are fundamental.

Recognize it and prioritize it

End-to-end encryption combined with sufficient privacy insurance can provide a business, its stakeholders, and its customers with the safeguards needed to protect personal data from the risk of a data breach and the resultant financial impact. The first step for any company however, that handles large amounts of client data has to be prioritization of the risk of this data being breached by an unauthorized party.

In our increasingly connected society a data breach has as much, if not more, potential to inflict significant even fatal financial and reputational damage than any conventional risk facing a business today.

For more details on how to manage your exposure to risks associated with a data loss, contact:

US

Jim Whetstone

+1 312 239 6354

jim.whetstone@hiscox.com

International

Matthew Norris

+44 (0) 207 448 6756

matthew.norris@hiscox.com

www.hiscox.com/usa

Care has been taken to ensure the accuracy of information within this report but the publishers cannot accept responsibility for errors or omissions.

This communication provides general information on Hiscox's products and services only and is not intended to be, and does not constitute, a solicitation of business by syndicates at Lloyd's of London from or in respect of the USA and US territories. Inquiries as to insurance or other products or other services from US residents should be directed to an insurance agent or broker licensed to conduct business in the relevant US state.

6281 04/09