
Client Data Policies and Practices of Bloomberg L.P.

August 20, 2013

**Hogan
Lovells**



1.	INTRODUCTION	1
2.	SCOPE AND METHODOLOGY	3
	A. Retrospective Review	3
	B. Review of Client Responses and Public Statements	4
	C. Review of Current Client Data Compliance Framework.....	4
	D. Review of Enhancement Plans	5
3.	SUMMARY OF FINDINGS AND RECOMMENDATIONS.....	6
	A. Journalist Access to Client Data via UUID and ADSK	6
	B. Journalist Use of Other Terminal Functions	8
	C. The Message Posting.....	9
	D. Client Responses and Public Statements	10
	E. Current Client Data Policies and Practices	11
	F. Enhancement Plans	13
4.	BACKGROUND	14
	A. Bloomberg’s Business and Culture	14
	B. The Events of Spring 2013	15
5.	RETROSPECTIVE REVIEW	17
	A. Journalist Access to UUID and ADSK Functions	17
	B. Journalist Access to Other Functions Containing Client Data.....	35
	C. The Message Posting.....	41
6.	REVIEW OF CLIENT RESPONSES AND PUBLIC STATEMENTS	46
	A. Objectives and Scope.....	46
	B. Methodology	46
	C. Findings and Recommendation.....	47
7.	REVIEW OF CURRENT CLIENT DATA POLICIES AND PRACTICES	49
	A. Objectives and Scope.....	49
	B. Assessment of Overall Client Data Compliance Framework	51
	C. Review of Enhancement Plans	80
8.	Appendices	85
	Appendix A: Hogan Lovells and Promontory’s Terms of Reference	85
	Appendix B: Statement of Samuel J. Palmisano, Independent Advisor to the Board of Directors of Bloomberg L.P., on the Hogan Lovells/Promontory Report.....	87
	Appendix C: List of Recommendations	88
	Appendix D: Mr. Doctoroff’s Blog Posts Addressing Client Data Issues.....	94
	Appendix E: Mr. Winkler’s Opinion Piece.....	98
	Appendix F: Bloomberg’s Client Data Principles.....	100

1. INTRODUCTION

In May 2013, Bloomberg L.P. (“Bloomberg”) engaged Hogan Lovells US LLP (“Hogan Lovells”) and Promontory Financial Group LLC (“Promontory”) to review Bloomberg’s current practices and policies related to the treatment of data Bloomberg collects and compiles from and about its clients and terminal users (for purposes of this report, “Client Data”)¹ as well as past data access issues recently raised by Bloomberg’s clients. The terms of reference governing our engagement are attached as Appendix A.

Bloomberg engaged Hogan Lovells and Promontory in response to concerns that prior to April 19, 2013, Bloomberg policy had permitted journalists in Bloomberg’s News and Multimedia divisions to access certain data relating to how Bloomberg clients used Bloomberg’s core product, the Bloomberg Professional service (a real-time financial information service and platform popularly known as “the terminal”). A report that a former Bloomberg employee had posted private client messages on a website accessible via the Internet (the “Message Posting”) also prompted our engagement.²

Bloomberg’s Board of Directors also engaged Samuel J. Palmisano, former Chairman and CEO of the IBM Corporation, as an independent advisor on data security and privacy. We met regularly with Mr. Palmisano and presented him with our methodology, findings, and recommendations; he provided us with advice and direction. Mr. Palmisano’s statement on this Report is attached as Appendix B.

Concurrent with our review of Bloomberg’s Client Data practices, Clark Hoyt, former editor-at-large at Bloomberg and public editor of the *New York Times*, reviewed the relationship between Bloomberg’s news and commercial operations and Bloomberg’s current news practices regarding Client Data privacy and confidentiality. We met regularly with Mr. Hoyt, whose review involved interviewing approximately 200 individuals. When Mr. Hoyt’s review identified potential instances of past journalist access to Client Data, we assessed them and incorporated our findings into this Report.

During the course of Hogan Lovells and Promontory’s review, teams of attorneys, data security and privacy professionals, technical analysts, and consultants from our firms used their legal, regulatory, governance, compliance, and technical experience to:

¹ The term “Client Data” does not include aggregate readership statistics and other similar data that do not identify individual terminal users or clients (e.g., the number of terminal users who have read an article, without identifying the terminal users or the firms with which they are associated).

² Where used in this Report “we,” “our,” and “us” refer to Hogan Lovells and Promontory jointly.

- Document whether, why, how, and to what extent Bloomberg journalists had been allowed to access data relating to how Bloomberg clients used Bloomberg products;
- Review the Message Posting and assess the nature of the messages posted by the former employee;
- Review Bloomberg's responses to clients regarding journalist access issues and the Message Posting;
- Assess and test Bloomberg's current information security and privacy practices; and
- Advise Bloomberg on its plans to further enhance its security and privacy controls.

Our mandate also included preparing this Report, which summarizes the work we performed, the methods we used, our findings, and our recommendations, to support Bloomberg's goal to become an industry leader with respect to data policies and practices.

Our list of recommendations is attached as Appendix C.

Bloomberg cooperated fully with our review, providing us open access to its personnel, documentation, information systems, and facilities. Where appropriate, Hogan Lovells and Promontory coordinated this review with Bloomberg and its internal and other external counsel. In conducting our review, we relied at times upon the expertise and work of Bloomberg personnel and acknowledge in particular the assistance and cooperation of Bloomberg's Client Data Compliance Officer and Bloomberg's Head of Security, as well as personnel working under their direction. In many instances, we were able to verify information provided by Bloomberg and have so noted in this Report. In other instances, we relied upon the presumed accuracy of information Bloomberg provided.

Bloomberg made clear to us its commitment to go beyond minimum legal requirements and to establish leading practices for the privacy and security of Client Data. We found Bloomberg to be open to our recommendations, and Bloomberg has dedicated significant resources to incorporating new controls into its Client Data compliance framework.³ Bloomberg has implemented or agreed to implement the recommendations we made.

This Report reflects Hogan Lovells's and Promontory's joint and separate⁴ findings, conclusions, recommendations, and advice pertaining to Bloomberg's Client Data practices.

³ This framework consists of tone at the top, governance, internal controls including policies and procedures, training, and accountability mechanisms.

⁴ Where work performed during the course of the review or findings, conclusions, recommendations, or advice contained in the Report should be attributed solely to either Hogan Lovells or Promontory and the individual firm's involvement is not otherwise clear from the context, we indicate that by using the name of the appropriate firm.

We permitted Bloomberg to review this Report in draft form to identify factual errors for our consideration.

2. SCOPE AND METHODOLOGY

A. Retrospective Review

The retrospective portion of our review examined Bloomberg journalists' prior uses of Client Data via certain terminal functions as well as the Message Posting. In conducting our review, we:

- Reviewed the available data to determine whether, prior to April 19, 2013, Bloomberg journalists accessed Client Data via terminal functions. Specifically, we reviewed journalist access to both online help desk chat sessions (“ADSKs”) and terminal user profiles (“UUIDs”). Because of the freeform text that terminal users could input into their help desk chat sessions, we examined all ADSKs within the data set we used for our review to determine whether those ADSKs had been viewed by journalists. Because of the limited types of data present on UUID screens, we reviewed a large, representative sample of UUIDs that available logs indicated had been viewed by journalists. We subsequently interviewed journalists to develop an understanding of UUID, ADSK, and journalist use of the terminal.
- Determined, to the extent practicable and from the data available, whether particular instances of journalist access to Client Data via UUID or ADSK could be linked to a news article published by any Bloomberg journalist in the two weeks after the access.
- Reviewed the Message Posting and assessed the extent to which the former employee misappropriated or disclosed Client Data.
- Reviewed other reports and concerns that arose during our review, that were related to journalists accessing Client Data during newsgathering activities via terminal functions (other than UUID and ADSK), and that presented the possibility of significantly impacting Bloomberg or its clients.

Bloomberg did not have a policy or practice of maintaining comprehensive logs of employee access to UUID or ADSK and did not perceive a business reason to do so. To support our review, Bloomberg performed a comprehensive search for available logs and was able to assemble access data from a number of sources, the integrity of which was validated by comparing it to other data logs. While no single source provided a complete record of access, the ADSK and UUID logs, validated by other data sources, provided a reasonable sample for

our review. As discussed in more detail below, the logs used in our review covered roughly two weeks out of each month for the period from June 2012 to April 2013.

The retrospective elements of our review were limited to the issues listed above.

B. Review of Client Responses and Public Statements

In assessing the accuracy of Bloomberg's public statements and Bloomberg's written communications to clients about its Client Data practices, we:

- Obtained Bloomberg's public statements, general statements offered to clients in updates, and communications addressing specific client concerns that were issued prior to our engagement;
- Reviewed those communications and later such communications for assertions about Bloomberg's current or past practices or controls relating to Client Data, and evaluated those assertions against available evidence;
- Worked with Bloomberg during the course of our engagement to construct a framework for preparing appropriate public statements and communications to clients, including, in many instances, providing drafting assistance (Hogan Lovells) and evaluating assertions against available evidence prior to release (Promontory); and
- Considered whether Bloomberg issued accurate updates to clients when new information warranted updating previous statements, and evaluated Bloomberg's updates against available evidence.

C. Review of Current Client Data Compliance Framework

We assessed Bloomberg's current Client Data compliance framework, including:

- Tone at the top;
- Governance;
- Internal controls, including policies and procedures, in terms of their design, content, and implementation;
- Ongoing employee training; and
- Accountability mechanisms.

When assessing the implementation of the internal controls in place, Promontory performed a range of tests, sometimes sampling different systems on the basis of risk or on a random basis. For most of this testing, we used a separate team of personnel who had not previously

been involved in providing advice to Bloomberg. In developing our tests, we made reference to various standards:

- The guidelines established by the Federal Financial Institutions Examination Council (“FFIEC”);
- The International Organization for Standardization 27000 series (“ISO 27000”);
- The Control Objectives for Information and Related Technology (“COBIT”);
- National Institute of Standards and Technology Special Publication 800-53 (“NIST 800-53”);
- The Information Technology Infrastructure Library (“ITIL”); and
- Our knowledge of industry leading practices and regulatory expectations for service providers working with regulated financial institutions.

Promontory’s work in reviewing these areas included:

- Interviewing over 225 Bloomberg employees;
- Reviewing over 350 documents relating to Bloomberg’s Client Data policies and practices;
- Reviewing over 500,000 Bloomberg News (“News”) articles to assess whether and how Client Data may have been used in the course of newsgathering; and
- Performing over 230,000 separate tests of Bloomberg’s access controls and other controls relating to information security.

All work performed was subject to a separate quality assurance review.

D. Review of Enhancement Plans

We also reviewed Bloomberg’s future plans to enhance its Client Data compliance framework and component controls to determine whether those plans:

- Provide for reasonable and appropriate enhancements;
- Address our recommendations;
- Reflect appropriate priorities; and
- Can feasibly be completed within the specified timeframes.

3. SUMMARY OF FINDINGS AND RECOMMENDATIONS

Our review found that prior to April 19, 2013 Bloomberg permitted journalists to access a limited subset of Client Data in the course of their work; Bloomberg management has demonstrated that it understands the seriousness of its responsibility to safeguard and use Client Data appropriately; and after Bloomberg management recognized the need to change Bloomberg's policy regarding journalist access to Client Data, Bloomberg's control environment, as detailed in this Report, has undergone rapid and significant formalization and improvement.

At the start of our work in May 2013, we found that Bloomberg had already taken steps to tighten access restrictions and improve its overall approach to managing access rights. Since then, Bloomberg has worked to formalize and enhance its documentation of Client Data policies and procedures, in many instances drawing upon existing practices, and has implemented or agreed to implement all of our recommendations. We have reviewed the current Client Data policies and procedures and tested the key controls implementing them. Although we have identified opportunities for further enhancement of these controls, which are detailed in this Report and attached as Appendix C, we found that the overall Client Data compliance framework is appropriate, that key controls have been implemented as of the date of this Report, and that Bloomberg has committed to further enhancing its controls as demonstrated by its communications, approval of plans to hire additional resources for control enhancements, and other actions.

Our principal findings with respect to each of the main areas of our review are as follows:

A. Journalist Access to Client Data via UUID and ADSK

Prior to April 19, 2013, Bloomberg permitted journalists to access via UUID and ADSK a limited subset of Client Data related to terminal users. This subset included:

- For UUID, the date of account creation; certain contact, firm, and job role details about the terminal user; the terminal user's login creation date and login history; and the terminal user's most commonly accessed functions over the past week (without any information about the specific content accessed or generated while using the functions); and
- For ADSK, the contents of the terminal user's help desk requests in chat sessions between the terminal user and Bloomberg personnel.

For both UUID and ADSK, the screens do not provide information regarding specific financial holdings or positions unless a terminal user included that information in an ADSK during a chat session.

Journalist access to UUID and ADSK arose not as a result of a lapse in controls, but because of Bloomberg's longstanding policy that permitted journalists to have that access.

In reviewing access to ADSK, using roughly 24 non-contiguous weeks of data available from June 2012 to April 2013,⁵ Promontory found no articles that appear to have been based on information that a journalist may have obtained by viewing Client Data via ADSK. This finding is consistent with the results of the interviews of journalists and other Bloomberg personnel conducted by Hogan Lovells, which indicated that journalists made very limited use of ADSK (e.g., to assist in client inquiries, for sales purposes, and to research the backgrounds of individuals who could provide information for articles).

In reviewing access to UUID, using a large, representative sample of journalist UUID views from the roughly 24 non-contiguous weeks of data available from June 2012 to April 2013, Promontory examined Bloomberg news articles that i) were published within two weeks following a journalist accessing a UUID screen and ii) mentioned the name of the terminal user associated with the UUID or the associated client. Because it was difficult to determine whether an article originated from a journalist's review of a UUID screen solely by reviewing the data available, Hogan Lovells used the data and articles as background information to guide its interviews of journalists.

Regarding access to UUID, Hogan Lovells's interviews confirmed that a number of journalists had previously used their access to the UUID screen to do one or more of the following: i) look up a terminal user's contact or biographical information; ii) check a terminal user's last login to see if that data suggested that the user was no longer working for the client associated with the terminal; and iii) check if a user was logged on in order to optimize the likelihood that a terminal user was available before calling the user. In addition, a small number of journalists mentioned that they used UUID to identify the frequency with which terminal users accessed particular terminal functions (for purposes of sales or for developing sources); those who did mention using UUID access for that purpose also mentioned that it was not particularly effective for that use.

Hogan Lovells's interviews also indicated a widespread understanding that Bloomberg's sourcing policies did not permit UUID data to be used as a sole source for published articles. We found it noteworthy that the only known instance of a Bloomberg journalist disclosing the

⁵ With regard to the data used to identify journalist access, Bloomberg used UUID and ADSK logs, validated against various data extracts from its systems to build a database to support our review. No single source provided a complete record of access. As discussed in more detail below, the data used in our review covered roughly two weeks out of each month for the period from June 2012 to April 2013.

use of UUID in reporting occurred in 2011 when a Bloomberg Television anchor shared a terminal user's last login data during a telecast.

Bloomberg now prevents journalist access to UUID and ADSK⁶ screens. Those restrictions and our testing of them are discussed in Section 7, which addresses the current state of Bloomberg's Client Data compliance framework.

B. Journalist Use of Other Terminal Functions

During the course of our review, we received information about journalists using functions other than UUID and ADSK in the course of newsgathering. We determined that five of these reports warranted further review. Of these, we found that two were substantiated in part.

In the first, we identified one instance in which journalists had access to information regarding a planned offering of a mortgage-backed instrument. That information was accessible to all Bloomberg employees, but non-employees required a password to access it. A Bloomberg reporter used this information to publish a short description of the instrument. The reporter and editor responsible for the description stated that they did not know that the information was not available to all terminal users. Prior to our engagement, Bloomberg became aware of this access issue and promptly corrected it. Journalists no longer have access to such data. Bloomberg has taken appropriate personnel actions in order to reinforce the importance of protecting Client Data and using sound judgment when gathering information for articles.

In the second, we assessed reports that journalists were given access to an anonymous chat room set up for commodities traders. Like any other participant, reporters were able to view the chats without identifying themselves. While participants in an anonymous chat room likely understand that their comments are available to a broad and unknown audience, some participants in the anonymous commodities chat room may not have assumed that Bloomberg reporters were viewing the chats. We recommended that in the future, Bloomberg either explicitly notify terminal users of journalist participation in anonymous chats or exclude journalists from participation. Bloomberg has decided to exclude journalists from participation in anonymous chats and has already implemented measures to enforce this policy change.

In addition, we reviewed three other reports of possible journalist access to Client Data, and we found that they were either unsubstantiated or did not involve improper access to Client Data.

⁶ ADSKs related to News (e.g., ADSKs raising questions about articles) are forwarded to trainers in the News division, and they may forward questions or issues raised in those ADSKs to journalists as appropriate.

In the first, we examined and assessed whether journalists might have had access to a sales database maintained by Bloomberg. The sales database at issue is used by Bloomberg sales personnel to record information regarding prospects and terminal users, and to maintain records regarding sales contacts and conversations. We found from the data available to us that a limited number of journalists had access to the database, and no journalists have had access since May 1, 2013. Hogan Lovells's interviews with journalists did not provide any indication the database was ever used as a source or lead for an article, and we did not find any evidence for this elsewhere.

In the second, we assessed whether journalists might be able to use the terminal to view directly what specific articles terminal users were reading. It was possible prior to May 12, 2013 for journalists to use a function that allowed Bloomberg employees to view data, aggregated at the client level (not at the level of an individual user), to learn about what articles a client's terminal users were viewing. We found no evidence that journalists used this function in the process of newsgathering, and the function was disabled for all employees on May 21, 2013.

In the third, we assessed whether the terminal allows journalists to access ratings reports from analysts. In response to such concerns, we reviewed whether journalists used the terminal to obtain analyst reports that were intended for limited viewership. We found no evidence that journalists were able to do so without having been authorized by administrators at the entities that generated the reports.

C. The Message Posting

Bloomberg first learned about a former employee's posting of files containing client messages on May 13, 2013, when the *Financial Times* ("FT") notified Bloomberg that the FT was about to publish an article about the Message Posting.

Bloomberg engaged outside counsel from Willkie Farr & Gallagher, LLP ("WFG"), who in turn engaged the forensics firm Stroz Friedberg, LLC to conduct a review. Through this review, Bloomberg learned that the former employee posted three files to the Internet containing messages from August 28, 2009, September 10, 2010, and the week of September 6-10, 2010. The former employee who posted the files cooperated with WFG's review. He stated that he did not recall precisely when he posted the messages, and he believed he did so within the few weeks following August 28, 2009 and September 10, 2010. The former employee reportedly intended to upload the files to a private server, and he stated that he did not remember when the files were made publicly available. He represented that he discovered that the files were publicly available only after a reporter called him on May 13, 2013, and told him that an article was being written about the posting of the files.

The former employee told WFG that he intended to transfer the files to private servers outside of Bloomberg because he wanted to analyze the messages they contained in a manner that exceeded his permitted abilities on Bloomberg systems. He also stated that he wanted to convince Bloomberg's senior management of the viability of his idea for further developments to Bloomberg's message-scraping product, which allows clients to use Bloomberg technology to extract pricing information from messages that clients receive via the terminal.

In transferring the files outside of Bloomberg and posting them on a public website, the former employee violated Bloomberg's policies.

Well in advance of Bloomberg's discovery of the Message Posting, Bloomberg had already undertaken efforts to enhance its controls around employee data transfers. Since learning of the Message Posting, Bloomberg has taken additional steps to enhance its controls around systems that access or house Client Data. As detailed in our assessment of Bloomberg's Client Data policies and procedures, we found that Bloomberg's current Client Data policies and practices are reasonably constituted to safeguard Client Data, are supported by key controls that our testing found to be appropriately designed and implemented, and will be strengthened with planned enhancements.

D. Client Responses and Public Statements

Promontory and Hogan Lovells assessed the accuracy of Bloomberg's public statements and Bloomberg's written communications to clients about its Client Data practices. These statements and communications included public comments of Bloomberg executives, general update letters to clients, and specific responses to individual client inquiries.

In all of the written communications we reviewed, we found Bloomberg's representations to clients regarding journalist access to Client Data and the Message Posting to be accurate except for one immaterial inaccuracy described later in this Report.

E. Current Client Data Policies and Practices

Our review found that, as of the date of this Report, Bloomberg has a Client Data compliance framework that includes:

- **Tone at the Top.** Bloomberg executives establish a tone at the top through communications to employees and clients emphasizing the importance of respect for Client Data and the need for robust and well-documented information management and security controls. In addition to reviewing these communications, we observed executives reiterate the issues in smaller meetings. Executives reinforced their communications with actions, including the allocation of resources to enhance controls. We found that the tone at the top is also reflected in the communications and actions of managers beneath the executive level. Our interviews further established that line employees understand and share the views of senior management on the importance of respect for Client Data and the need for robust and well-documented information security controls. We did not observe any instance in which the tone established at the top was not shared by a Bloomberg employee.
- **Governance.** Bloomberg manages its Client Data compliance framework through managerial responsibility, a dedicated Client Data Compliance Officer, and Board oversight (including a newly established Audit, Risk & Compliance Committee of the Board of Directors comprised of a majority of independent directors). Bloomberg has approved plans and taken steps to enhance audit, risk, systems, and compliance resources.
- **Internal Controls.** Bloomberg has adopted a suite of foundational Client Data principles, policies, and procedures that it has committed to reviewing and updating on a periodic basis. Promontory tested the effectiveness of key controls implementing these policies and procedures and found them generally to be effective, with exceptions and recommended improvements noted in the Report.
- **Training.** Bloomberg recently launched an Information Security Training Program for all Bloomberg personnel that incorporates the requirements of Bloomberg's Client Data Principles and its underlying policies. The first phase of this training includes four modules targeted at managers, human resources staff, Business Administrators for Roles ("BARs") (i.e., business staff that administer access permissions), and managers in Research & Development ("R&D") with access control authority. The content of this training will be adapted for a broader audience of all Bloomberg personnel.

- **Accountability.** Bloomberg has directed its head of human resources to include risk and compliance objectives, including Client Data compliance objectives, into the performance evaluation process for appropriate personnel. Bloomberg is taking action with respect to personnel who violated policies that existed at the time of their respective violations.

Our Report includes 54 recommendations to enhance this framework. These recommendations are described in each section of the Report and a consolidated list of them is attached as Appendix C. Bloomberg has agreed to implement all of these recommendations and, in many cases, has recently completed or begun to implement them. Examples of important recommendations include:

- Implementing planned and recommended data-access and end-user permissioning enhancements;
- Increasing internal audit, risk, systems, and compliance resources; and
- Tracking the status of Bloomberg's efforts to implement these recommendations and using Internal Audit and, as needed, external resources to validate that the recommendations are fully implemented.

Bloomberg has expressed a commitment to the continuous improvement of its Client Data compliance framework by implementing enhanced monitoring, testing, auditing, and third-party reviews.

In summary, we found that Bloomberg's current Client Data policies and practices are reasonably constituted to safeguard Client Data, are supported by key controls that our testing found to be appropriately designed and implemented, and will be strengthened with planned enhancements. We conclude that Bloomberg has an appropriate Client Data compliance framework in place that:

Key Items
Prevents journalist access to confidential Client Data:
Journalists no longer have access to client UUID and ADSK screens. ⁷
Journalists do not have access to functions that permit access to Client Data relating to securities, positions, and orders.
Journalists no longer have access to Bloomberg's anonymous chat rooms.
Includes appropriate training on privacy and Client Data compliance policies and procedures:
Firm-wide training on privacy and Client Data issues is supplemented with tailored training modules for specific workforce roles.
A central portal provides access to training modules as well as privacy and Client Data policies and procedures.
Enhances Bloomberg's prior Client Data compliance controls, including:
A role-based permissioning framework.
A centralized access control team that oversees the granting of access privileges to restricted data.
Systems that monitor for unauthorized access by employees.
A framework that formalizes Client Data compliance policy and procedures.
Enhances governance, including:
An Audit, Risk & Compliance Committee of the Board that is comprised of a majority of independent directors.
The appointment of a Client Data Compliance Officer in April 2013.
Plans to hire a Chief Risk and Compliance Officer and increase audit, risk, systems, and compliance resources.
An expressed commitment to undergo periodic third-party reviews of Client Data compliance controls, the results of which will be made available to clients.

Our findings and recommendations are further detailed in the body of this Report.

F. Enhancement Plans

We had the opportunity to make recommendations and assist Bloomberg in the formulation of its enhancement plans. Bloomberg was receptive to our input, and we find that the resulting plans:

- Provide for reasonable and appropriate enhancements;
- Address our recommendations;
- Reflect appropriate priorities; and
- Are feasible to complete in the specified timeframes.

⁷ ADSKs related to News (e.g., ADSKs raising questions about articles) are forwarded to trainers in the News division, and they may forward questions or issues raised in those ADSKs to journalists as appropriate.

4. BACKGROUND⁸

A. Bloomberg's Business and Culture

Launched in 1981, Bloomberg is now a leading provider of global financial and business information and news.⁹ The terminal is the core of Bloomberg's business, providing a mix of data and analytics regarding fixed income instruments, equities, currencies, commodities, mutual funds, and industry sectors. Terminal users can also access regulatory filings, legal documents, and biographies. Since 1990, when Bloomberg launched Bloomberg News, News's articles have been readily accessible via the terminal. Bloomberg Industries ("BI") offers data, analytics, and reports regarding over 100 industries and major sectors via the terminal. The terminal provides an email and messaging system that allows all terminal users to communicate with each other without having to exit the terminal interface. And the terminal provides access to Tradebook, which offers Bloomberg clients trading solutions on over 100 global exchanges. In recent years, the terminal has added coverage of legal, government, and regulatory matters.

As a result of the evolution of the terminal and its overall business, Bloomberg's clients entrust Bloomberg with access to a considerable amount of data.

From its inception, Bloomberg's culture has emphasized rapid and responsive customer service and product development.¹⁰ Based on our interviews, we understand that in order to facilitate the delivery of customer service, Bloomberg traditionally allowed all employees, including journalists, to access and respond to client help desk requests. Interviewees stated that Bloomberg has a flat organizational structure, which eschews formal organization charts and encourages employees to disregard silos in order to respond to client needs and opportunities as they arise. Bloomberg employees often "wear many hats." A visible manifestation of Bloomberg's culture is the open work environment – there are no offices – and collaboration is encouraged via seating and traffic patterns.

Based on our interviews, we understand that Bloomberg journalists often attended, and sometimes continue to attend, sales calls, especially in Bloomberg's smaller offices. That practice aligned with Bloomberg's culture of collaboration and the flat organizational structure. Bloomberg traditionally has encouraged journalists to learn about client needs and to educate

⁸ This section is based on published works about Bloomberg as well as interviews with Bloomberg personnel.

⁹ See *Company Overview of Bloomberg L.P.*, Bloomberg Businessweek, <http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapid=160210>.

¹⁰ Bloomberg's culture emphasized the core business and client service, and actively discouraged actions that could be viewed as bureaucratic. See Jeremy Dann, Bloomberg L.P., a 1999 Harvard Business Review Case Study.

clients about Bloomberg's news and information services. According to Bloomberg management and the Bloomberg journalists Hogan Lovells interviewed, one of the ways that journalists learned about client needs prior to April 19, 2013 was to review how clients were using the terminal. Prior to April 19, 2013, journalists were allowed to access limited data about client terminal usage ("limited Customer Relationship Management data" or "limited CRM data") through certain terminal features, namely UUID and ADSK.

B. The Events of Spring 2013

On April 16, 2013, a Bloomberg reporter called the Hong Kong office of a Bloomberg client and inquired as to whether an individual affiliated with the client's firm had recently left the firm. According to the client, the reporter noted that the individual affiliated with the firm had not logged into the Bloomberg terminal for some time. The client contacted Bloomberg to complain that Bloomberg journalists appeared to have access to data about terminal usage. Bloomberg management examined the client's concerns and responded by changing Bloomberg's Client Data access policies so that journalists would have access only to the same Client Data that is available to all clients (e.g., a terminal user's Bloomberg.net email address).¹¹ As a result, starting on April 19, 2013, Bloomberg began to shut off access for all journalists in its News and Multimedia divisions to the functions that formerly provided them with access to Client Data not available to all terminal users.

On May 9, 2013, the *New York Post* reported both Bloomberg's decision to restrict journalist access to limited CRM data and the previously mentioned client's complaint regarding how a journalist appeared to have used that data.¹² The *New York Post* article was followed by articles in other news outlets.

On May 10, 2013, Bloomberg received its first customer request for information relating to the issue of reporter access to Client Data. On that same day, Bloomberg CEO and President Daniel Doctoroff sent a note to Bloomberg subscribers stating, "Although we have long made limited customer relationship data available to our journalists, we realize this was a mistake."¹³ Mr. Doctoroff announced that Bloomberg had centralized its Client Data protection and security efforts in April 2013 by creating the position of Client Data Compliance

¹¹ The exception to this is that Bloomberg journalists can view readership information aggregated over all terminal users (e.g., how many terminal users have viewed an article) that does not identify which terminal users read an article or which clients employ those terminal users. This information is not available to terminal users not employed by Bloomberg

¹² Mark DeCambre, *Goldman Outs Bloomberg Snoops*, N.Y. Post (May 9, 2013), http://www.nypost.com/p/news/business/goldman_outs_bloomberg_snoops_ed7SopzVLaO02p9foS7ncM.

¹³ Daniel L. Doctoroff, *Safeguarding Client Data*, Bloomberg Blog (May 10, 2013), <http://blog.bloomberg.com/2013-05-10/safeguarding-customer-data/>.

Officer, which is responsible for managing the policies and procedures relating to access to Client Data. A senior executive was appointed to the position.

Over the next few days, Peter Grauer, Bloomberg's Chairman of the Board; Mr. Doctoroff; and other Bloomberg executives contacted more than 300 clients to apologize and to explain that reporters were able to access only limited CRM data. On May 13, 2013, Mr. Doctoroff started a blog to facilitate direct communications with Bloomberg's clients, employees, and partners. In his initial blog post, Mr. Doctoroff encouraged all of Bloomberg's subscribers to contact him directly should they have any questions or concerns. Mr. Doctoroff emphasized that journalists did not have access to messaging, trading, portfolio, monitor, blotter, or other related systems.¹⁴

Matthew Winkler, editor-in-chief of Bloomberg News, published an opinion piece on Bloomberg View, Bloomberg's editorial and commentary page, on May 13, 2013. In that piece, Mr. Winkler said that reporters should not have access to proprietary client data and that it was an inexcusable error to allow that access. He stated that reporters at no time had access to trading, portfolio, monitor, blotter, or other related systems, and that reporters could not access clients' messages to each other or the specific articles or securities viewed by clients.¹⁵

On the same day that Mr. Doctoroff started his blog and Mr. Winkler published his opinion piece, the *FT* reported that a former Bloomberg employee had posted to a public website files containing over 10,000 private messages sent between Bloomberg terminal users. Bloomberg received its first request for information regarding the posting of the messages by May 15, 2013.¹⁶

Bloomberg announced on May 17, 2013 its appointment of Samuel J. Palmisano, former Chairman and CEO of the IBM Corporation, to serve as an independent adviser regarding Bloomberg's privacy and data standards. On the same day, Bloomberg announced that it had hired Hogan Lovells and Promontory to conduct a review of those policies and practices. Bloomberg also announced on May 17, 2013 that Bloomberg had asked Mr. Hoyt, former Editor-at-Large at Bloomberg News and former public editor of the *New York Times*, to review the relationship between Bloomberg News and Bloomberg's commercial operations. During the course of our review, Bloomberg provided public updates as to the progress of the review and responded to customer requests for information.¹⁷

¹⁴ Mr. Doctoroff's blog posts addressing Client Data issues are attached in Appendix D.

¹⁵ Mr. Winkler's opinion piece is attached in Appendix E.

¹⁶ More information regarding the Message Posting is contained in Section 5.C.

¹⁷ See Dan Doctoroff, *The Latest from Our CEO*, Bloomberg, <http://blog.bloomberg.com/ceo/>.

5. RETROSPECTIVE REVIEW

Our review of Bloomberg's prior uses of Client Data ("Retrospective Review") focused on the issues raised by reports of i) journalist access to Client Data and ii) the Message Posting. As to those reports we reviewed, our scope was focused on understanding how that past activity impacted our assessment of Bloomberg's current Client Data Policies and practices. In reviewing journalist access issues, we focused on assessing whether and to what extent Bloomberg journalists used Client Data in creating news articles. We began by looking at the specific internal functions that journalists reportedly used to access limited CRM information about terminal usage. Those functions, UUID and ADSK, and our review of journalist access to those functions are described in Section 5.A. Section 5.B describes our assessment of reports of journalist access to other terminal functions providing access to Client Data. That assessment focused on determining whether the reported access existed and how journalists used that access. Section 5.C describes the results of our assessment of the Message Posting.

A. Journalist Access to UUID and ADSK Functions

Background

In reviewing Bloomberg's prior uses of Client Data, Hogan Lovells and Promontory focused on the issues raised by clients regarding Bloomberg's use of Client Data. In particular, we assessed whether and to what extent Bloomberg journalists used UUID and ADSK screens in the course of newsgathering.

- UUID is a customer relationship management ("CRM") and technical and customer support function that displays data about terminal users, including some data related to their terminal usage. Of particular relevance to our review, UUID provides four pieces of data that are unavailable to non-employee terminal users:
 - o When the terminal user created his or her login;
 - o The terminal user's job role and certain contact details;
 - o The terminal user's login history (including the last login); and
 - o Aggregate information about the most common functions that the terminal user accessed, not including specific content viewed via those functions. The UUID screen also provides access to the ADSK function, which is described below.

- ADSK provides a terminal user's history of help desk inquiries and is accessible both as a standalone function and through the UUID screen. Running the ADSK function on a terminal user provides access to the full text of the terminal user's help desk chat sessions from approximately the previous year. For most help desk requests more than one year old, ADSK reveals the initial help request and any handoffs of the request within Bloomberg. Each chat session is referred to as an "ADSK ticket."

With respect to UUID access, we first confirmed that the UUID screen provides access to limited data regarding terminal users (e.g., login data and aggregate information about functions used) but not specific, confidential data such as holdings. Given the limited data available via UUID and the extent of journalist access that occurred, we reviewed a large, representative sample of the available data relating to journalist UUID access during the period from June 2012 to April 2013.

With respect to ADSK, there were far fewer instances of journalist access. But each instance had greater potential for the disclosure of Client Data because ADSKs contain correspondence supplied by terminal users in free-text fields that could contain a wide range of information. We therefore examined all ADSKs within the data set we used for our review to determine whether they had been viewed by journalists.

Methodology and Objectives

Our review of journalist access to UUID and ADSK screens consisted of four phases:

- Phase 1: Reviewing and testing the extraction and formatting of the data sets from Bloomberg's systems that were used in the Retrospective Review.
- Phase 2: Reviewing a sample of instances of journalist UUID screen access from the data set available and then identifying "Examined Articles" (defined below) for those instances.
- Phase 3: Identifying all instances of journalist ADSK access from the data set available and then identifying Examined Articles for those instances.
- Phase 4: Interviewing journalists regarding access to UUID and ADSK screens. Most of these interviews were conducted following Phases 1-3, and were informed by the results of those phases. In all cases, information regarding journalists' access to UUID and ADSK screens during the period in scope was available to Hogan Lovells prior to the interview.

We used the findings of the testing to develop an understanding of how journalists likely used the UUID and ADSK functions before Bloomberg shut off journalist access to these functions. We made the findings available to Bloomberg to inform its discussions and communications with specific clients.

The approach to each Phase of testing and our findings are detailed later in this section.

Individuals Included in the Review

We defined which Bloomberg personnel were included in the Retrospective Review, referred to as “Newspersons,”¹⁸ by doing the following:

- Obtaining current staff lists for all employees in Bloomberg’s News, Multimedia, BI, and Bloomberg Briefs divisions;
- Reviewing the job roles of staff and excluding those staff whose roles appeared not to involve newsgathering activities; and
- Reconciling our list with Bloomberg’s list created in a parallel exercise.

We used this list in the subsequent review of UUID and ADSK screen access.

How We Defined “Examined Articles” for the Review of UUID and ADSK Usage

Promontory deemed an article to be an “Examined Article” within the scope of the review if:

- The article was published in the two-week period subsequent to a Newsperson’s UUID or ADSK access; and
- The article or article metadata (e.g., keywords associated with the article) mentioned the terminal user who was the subject of the UUID or ADSK access, or the client that employed that terminal user.

Our classification of a news item as an Examined Article does not in itself indicate that we discovered a link between the generation of that news item and a Newsperson’s access to a UUID or ADSK screen. We classified news items as Examined Articles solely on the basis of whether the items i) contained information mentioning a terminal user or a user’s employer and ii) were published within the two weeks following a Newsperson’s access to that terminal user’s UUID or ADSK screen. Indeed, as discussed below, Hogan Lovells’s interviews

¹⁸ As used in this Report, “Newspersons” refers only to those Bloomberg personnel satisfying the above criteria identified for the UUID and ADSK reviews. When we use “journalist” or “reporter,” we refer to those individuals satisfying the common definitions of those terms regardless of whether they satisfied the criteria for being labelled a “Newsperson.”

established that a substantive link between the data access and an Examined Article was very rare.

Data Available for the Review

Bloomberg conducted an extensive assessment of the data sets available that could lead to the identification of Newsperson access to terminal users' UUID screens or ADSKs. As described below, Bloomberg did not maintain logs of this data in a form well suited to an historical review of this type. Bloomberg did not have a policy of maintaining such logs and did not perceive a business reason to do so. The data set Promontory used to review Newsperson access to Client Data via UUID and ADSK was built from a number of sources. The data set consisted of data relating to roughly two weeks out of each month for the period from June 2012 to April 2013, which provided roughly 24 non-contiguous weeks of log data. Promontory reviewed and tested Bloomberg's data extraction and reconciliation processes.

Phase 1: Testing of Data Extraction-Methodology and Findings

Bloomberg identified a number of troubleshooting logs and backup sources that provided partial records of historic use of the UUID and ADSK functions. We reviewed those sources and agreed with Bloomberg that, on the basis of the scope and integrity of the data available, the AdskDbLogs backup provided the most appropriate source of data for a review of Newsperson access.

AdskDbLogs creates a record when terminal users click into the ADSK record from any ADSK screen to view a help desk chat transcript. The available backups of these logs also contained information about most usage instances of the UUID function because each variant of the UUID screen displays the date when the terminal user last created an ADSK ticket. The UUID screen displays this data by the function sending a request for the information to the ADSK function. When this occurs, the AdskDbLogs record that the terminal user accessed ADSK by running the UUID function. Bloomberg keeps this data to track database performance as a means of confirming the ongoing operation of the system.

The data in the AdskDbLogs backups were limited to a specific time window because Bloomberg writes data to AdskDbLogs on an ongoing basis (e.g., each time the primary database is queried). The log contains 13 to 14 days of data at any given time, with the oldest data being overwritten by new data. The log is backed up to tape once a month. Therefore, the backups contained roughly 24 non-contiguous weeks of data over the period from June 2012 to April 2013. For purposes of our review, Bloomberg uploaded the AdskDbLogs to a relational database and mapped the data against other logs. These other

data sources corroborated the information available for the UUID and ADSK views logged in the AdskDbLogs backups.

Promontory worked with Bloomberg to test the data sets for integrity, completeness, and appropriateness for the scope of the review. The work included:

- Reviewing the work of the Bloomberg team that mapped the ADSK tickets to calls made to a separate log of access to an instant messaging database, thereby independently affirming the ADSK database's integrity.¹⁹ This access log records when chat transcripts are requested by the ADSK function when the ADSK screen is viewed by a user. Matching the timestamps of ADSK requests to those of the chat transcript requests returned a correlation of 97.4% between timestamps for the ADSK tickets in the data set for the review and the timestamps for calls to the instant messaging database, within two seconds of the request. The instant messaging database was used to supplement the ADSK data as a source of chat transcripts to make a more complete record. This exercise gave us confidence that the ADSK dataset was a robust record of ADSK searches performed by Bloomberg terminal users.
- Reviewing the work of the Bloomberg team that had mapped the ADSK data against logs recording the total number of instances in which terminal users functions available via the terminal, including UUID total hit counts. Bloomberg captures a record of functions run by employees in a second database, which was used to create a "hit count" of UUID accesses by journalists. The number of UUID viewing instances reflected in the AdskDbLogs backups matched these hit counts for UUID, providing us an additional level of confidence that the AdskDbLogs backups constituted a robust record of Bloomberg terminal users' UUID searching. In addition, we validated the process Bloomberg used to validate usage statistics based on the serial numbers of journalists' terminals against function logs as an additional test of the AdskDbLogs' ability to capture UUID hits. This provided additional confidence in the integrity of the logs.

¹⁹ We also examined each instant message chat transcript associated with an ADSK reviewed. These instant message logs were available directly within the ADSK screen itself up to roughly a year after the ADSK creation date. In those instances in which instant message chat logs were generated as a result of an ADSK session (in a very small percentage of cases, the ADSK did not make use of instant messaging at all; thus, no instant message log was created) but were no longer available through the terminal, we obtained these transcripts from a historical database and analyzed these, as well.

Promontory interviewed the staff who performed the work described above and reviewed the work itself. Promontory's conclusion is that the data extraction was performed appropriately and that sufficient controls were in place to maintain the integrity of the data.

Phase 2: Testing of UUID Access

Methodology for UUID Testing

Promontory extracted data specific to UUID access. Promontory identified and reviewed a large, representative sample of Newsperson UUID accesses. Promontory judged a sampling methodology to be appropriate for the review because Promontory established through its own evaluation of the UUID accesses that the type of data that a journalist could see on a UUID screen was limited and the data available contained a large number of UUID accesses. After conducting this analysis, Promontory compared its findings with the information that Hogan Lovells obtained during its interviews of journalists. Because the findings of the two processes were consistent, Promontory took additional comfort that the sampling approach was reasonable.

In the sample of UUID screen accesses, for every instance of a Newsperson viewing a terminal user's UUID screen, Promontory:

- Obtained all Examined Articles; and
- Reviewed each Examined Article to determine whether Client Data accessed via the UUID view in question could have generated any part of the Examined Article.

Hogan Lovells used Promontory's analysis of UUID views to inform interviews of Newspersons regarding past practices. These interviews are discussed below. Promontory's analysis also informed discussions Bloomberg had with clients that inquired about past journalist access to their Client Data.

Phase 3: Testing of ADSK Access

In reviewing access to ADSK using roughly 24 non-contiguous weeks of data available from June 2012 to April 2013, we:

- Identified journalist ADSK views;
- Reviewed the ADSKs viewed by journalists to determine whether they contained potentially sensitive Client Data (defined below) included by terminal users who initiated the ADSKs;

- Obtained all Examined Articles (i.e., those identified as relating to the terminal user or client employing the terminal user and issued in the two weeks after the Newsperson viewed the ADSKs); and
- Reviewed each Examined Article to determine whether Client Data accessed via the ADSK could have generated any part of the Examined Article.

Methodology for Identifying ADSKs Containing Sensitive Client Data

The ADSK function contains free-text fields recording terminal users' help desk inquiries. Those fields may contain potentially sensitive Client Data depending upon what information a terminal user sent in an inquiry. For example, a terminal user could ask for help regarding how to look at a particular security, thereby revealing an interest in that security. In many cases, there were legitimate reasons for Newspersons to access ADSKs. For example, terminal users often pose questions about news articles through ADSK, and reporters may be contacted to help resolve those ADSK inquiries. Reporters would often access ADSK records to see how those inquiries were ultimately resolved. Some ADSK usage appeared to be appropriate, and many ADSKs contained only technical inquiries that did not reveal any substantive, non-public information about terminal users or clients. Therefore, to focus our review, we defined and identified "sensitive" ADSK information. In conducting the analysis described below, Promontory considered an ADSK inquiry to contain sensitive Client Data when the inquiry:

- Mentioned specific companies, tickers, securities, or indices beyond standard or generic indices such as S&P 500 or FTSE 100;
- Mentioned data specific to niche markets (e.g., Bureau of Labor Statistics on unemployment in a specific industry sector or a list of software companies in Germany); or
- Was initiated by a high-profile individual (e.g., a CEO or other figure widely recognized in the financial industry).

Methodology for Reviewing Bloomberg News Articles Relating to ADSK Views

For every instance of a Newsperson viewing a client's ADSK inquiry containing sensitive Client Data ("ADSK Hit"), Promontory:

- Obtained all narrative content published by the Bloomberg newswire identified as relating to the client, and issued in the two weeks after the Newsperson viewed the Client Data; and

- Reviewed each Examined Article to determine whether Client Data accessed via the ADSK Hit in question could have generated any part of the Examined Article.

Hogan Lovells used information regarding Newsperson ADSK views to inform their interviews of Newspersons regarding past practices. These interviews are discussed below. Promontory's findings also informed Bloomberg's discussions with clients that inquired about past journalist access to their Client Data.

Phase 4: Interviews Informed by UUID and ADSK Testing

Scope and Methodology

Hogan Lovells interviewed Newspersons who were identified from the data available as having accessed UUID or ADSK information, as well as a sample of the managers and editors who supervised those Newspersons. The Newspersons Hogan Lovells interviewed included those Newspersons who most frequently accessed UUID and ADSK, and Newspersons selected at random. Fifty-eight of the interviews Hogan Lovells conducted were associated with the UUID and ADSK testing. For every interview, Hogan Lovells had a list of the Newsperson's UUID and ADSK views during the relevant time period as well as any Examined Articles potentially associated with those views. Hogan Lovells asked interviewees about those Examined Articles for which there was a potential connection.

For each interview, Hogan Lovells also questioned individuals about the following:

- Work history;
- Training at Bloomberg;
- General use of terminal functions;
- Specific use of UUID and ADSK;
- Whether and how they used terminal functions in newsgathering; and
- Whether they had access to various terminal functions that had the potential to convey Client Data.

In addition to the review of issues related to the UUID and ADSK data review, we examined the facts surrounding the Bloomberg News broadcast of certain information about UUID by a Bloomberg Television anchor in 2011. Hogan Lovells interviewed journalists and editors who were involved in the disclosure and the review that followed.

Journalist Use of UUID Function

Specific uses and frequency of UUID access. In the course of Hogan Lovells's interviews, Newspersons identified a number of specific ways that they used UUID function access. These included, in approximate order of frequency of use:

- Biographical and contact information. Many Newspersons who used UUID stated that the primary, and in many cases only, use for that access was to obtain background and contact information for individuals who were subjects of articles or provided information for articles. The Newspersons said that in some cases this information was available from publicly available terminal functions or public sources, but using UUID was quicker. In addition, UUID contact information sometimes included phone numbers or alternative emails that were not available on a terminal user's public profile.
- Last login information. Many of the Newspersons that Hogan Lovells interviewed acknowledged using UUID to view a terminal user's last login date and time. Newspersons offered two primary reasons for accessing this data. First, some Newspersons noted that they tried to avoid making unnecessary phone calls when contacting individuals, as they did not want to alert assistants or others that those individuals were communicating with Bloomberg reporters. By using UUID to see if an individual was logged into the terminal, Newspersons had a greater chance of reaching those individuals at their desks.

Second, Newspersons stated that they used UUID as part of their newsgathering process. Some of the heavy users of UUID acknowledged that it was a useful feature of UUID to be able to see when a potential subject of an article had last logged in. Several of the Newspersons interviewed said they used UUID login information to help them develop articles about the movement of financial firm employees. For example, several reporters said that if they received a tip that an individual had been fired or was leaving for another company, they would check UUID login data to see if there was any support for this tip. If UUID login data showed that the individual had not logged on for a period of days or weeks, the Newspersons would then proceed to look for additional information to confirm the initial tips.

Except for the episode involving a Bloomberg Television anchor that is discussed separately in this Report there was no indication that UUID login data served as a "cited source" or was approved as an "anonymous source" under Bloomberg's strict

sourcing rules.²⁰ None of the Newspersons Hogan Lovells interviewed, other than the anchor, indicated that they had ever used UUID data as a cited source. Each of the editors and team leaders with whom Hogan Lovells spoke denied that he or she had approved any article where UUID data was a cited or anonymous source. In most situations, Bloomberg News allows the use of anonymous sources only with the approval of the editor-in-chief, two executive editors, or two managing editors.²¹ Thus, we consider it unlikely that a Newsperson could have included UUID as an anonymous source without an editor's knowledge.

Both line reporters and editors viewed UUID login data as a convenient check on individuals providing information for articles. A few reporters did state that in rare instances, where sources were not particularly well known to editors or where there were doubts about a source's credibility, UUID login data could confirm information received from or about sources.

- Bloomberg signature. Terminal users can set up signatures for their accounts. These signatures are similar to auto-signatures on email platforms. When a terminal user's subscription is active, all Bloomberg Professional service users can view that terminal user's signature. When the subscription is deactivated, the terminal user's signature is not accessible to terminal users who are not Bloomberg personnel. However, Bloomberg employees with UUID access can access signatures associated with deactivated subscriptions for up to 90 days after the subscription is deactivated. Thus, if a terminal user had posted a departure notice as a signature, Newspersons with UUID access could have viewed the departure notice even when there was no longer public access to the terminal user's account or bio. Like login data, Newspersons used this data to help determine the employment statuses or locations of terminal users. We found no evidence that signatures were used as cited or anonymous sources in news articles. As noted previously, Bloomberg policy no longer permits journalists to access the UUID screens of clients' terminal users.
- User function frequency. Journalists, like other Bloomberg employees, could use UUID to view which functions terminal users accessed most frequently in the previous

²⁰ We define "cited source" as a reference identifiable from information in an article that supports information contained in the article. We define "anonymous source" as a reference that supports information contained in an article and cannot reasonably be identified by information contained in the article. One clear theme that ran through the interviews was the extensive and careful review of sourcing by editors and team leaders in the News division. Indeed, virtually every journalist we spoke to that had experience at other major newspapers or news organizations noted that Bloomberg's sourcing policy and the degree of review and control by editors was the strictest he or she had experienced.

²¹ Matthew Winkler, *The Bloomberg Way* 86 (2012) (a policy and style guide for reporters and editors).

week without being able to view the content accessed or input via those functions. For example, they could see that a terminal user had accessed an equity pricing function 25 times, but not the nature of the individual inquiries the terminal user made with the function or the individual securities that were viewed. Most of the Newspersons Hogan Lovells interviewed did not access or use this feature of UUID. Those Newspersons who did use the feature identified two potential uses for this data. Most commonly, the function was used as part of Bloomberg's sales and commercial operations. Journalists who were asked to accompany sales people on calls to terminal users would view the users' function usage to see the types of activities in which the users were engaged and what functions they accessed on a regular basis. This was supposed to allow journalists to develop articles or discuss potential articles with those terminal users. We note that this use of UUID was related to commercial activity and not newsgathering.

In addition, one Newsperson reported using this UUID data to identify terminal users who could be used as sources. For example, if a journalist was interested in finding potential sources at certain banks in a geographical location who traded in a particular group of commodities, the reporter could access UUID searches for a sample of terminal users to see who, if anyone, frequently accessed functions associated with those commodities. The reporter noted that this use of UUID was suggested by a trainer during the reporter's initial new-hire training. The reporter claims to have not used UUID in this way for long because the process was particularly time consuming and yielded little in the way of results.

Policies then in place. With regard to the types of UUID usage discussed above, we examined policies and procedures that were in place prior to April 2013. Under those policies and procedures there was no specific or general prohibition of any of these uses. There were confidentiality requirements imposed on journalists that governed disclosure of this data to third parties. The use of UUID data without affirmatively disclosing that data as a cited or anonymous source would not appear to violate these policies.

Connection between UUID access and article generation. We did not find any evidence that UUID last login data was used as a cited or anonymous source for any Examined Article. In the vast majority of cases we examined in the interviews, the Examined Articles identified had no substantive correlation to the UUID access. Hogan Lovells's interviews with the top users identified fewer than 10 unique articles for which Newspersons may have used UUID in newsgathering. In addition, some Newspersons with whom we spoke stated that while they could not remember using UUID in newsgathering for a specific article, they may have accessed a user's UUID during the newsgathering process. As discussed above, in no case

were we able to determine that UUID data was used as a cited or anonymous source for an Examined Article.

How journalists learned about UUID access. Many Newspersons interviewed said they received at least some training on UUID as part of their new-hire training. For the vast majority of Newspersons, this training consisted simply of an introduction to the function and how it worked. A few Newspersons were instructed by trainers on how UUID could be used for newsgathering as discussed in the discussion of uses above. The majority of Newspersons who used UUID searches in newsgathering said they learned the various capabilities of the function and its use in newsgathering from other journalists or editors. Newspersons reported that after new-hire training they received little formal ongoing training on the use of terminal functionality. Newspersons did recall receiving periodic training on libel and other areas of legal risk. Many reporters stated that it was not uncommon for the weekly notes from Matthew Winkler to contain discussions of ethics or newsgathering practices. These notes usually discussed style or praised reporters who had broken top articles. However, the notes would occasionally discuss prohibitions on certain practices. Based on Hogan Lovells's interviews, it appears that Newsrooms outside the United States were more likely to discuss these notes and developments at group meetings than U.S.-based newsrooms.

Terminal training for Newspersons was generally limited to how to use terminal functions. Other than new-hire training addressing confidentiality and not using Bloomberg information for personal use, Newspersons received little if any training on how terminal usage might affect issues relating to Client Data. We saw no evidence that the lack of training was the result of a deliberate attempt to avoid these issues. Rather, the absence of training on Client Data matters seems to have been due to lack of consideration or attention. Accordingly, the discussion below on policies and procedures emphasizes the need for continual and regular training enhancements.

Transparency of use. Hogan Lovells asked Newspersons whether there had been any restrictions placed on their above-described uses of UUID data and whether any concerns had been expressed at any level over the legitimacy or appropriateness of using UUID data in newsgathering. Newspersons did not report that they were aware of any attempt to restrict access to UUID prior to the events of April 2013. Only one Newsperson recalled discussions about whether the use of UUID by journalists was appropriate. In general, UUID use was either encouraged or viewed as a non-issue by editors and team leaders. Many Newspersons stated that the general view in the newsroom was that if journalists had access to a terminal function, it was appropriate to use that function for newsgathering. As discussed

below, this approach continued even after a Bloomberg Television anchor revealed UUID data on air in September 2011.

Many Newspersons did state that there was, at the very least, an understanding that journalists should not reveal to terminal users that journalists had access to UUID data. Most of the Newspersons who discussed this said that they either understood implicitly not to disclose UUID access or they learned this from discussions among newsroom staff. A small number of Newspersons said that at some point they were told explicitly by others to not reveal UUID access to terminal users. This is concerning in that it indicates that even though there was no policy against journalist access to UUID, there was an awareness before April 2013 and before the telecast in which a Bloomberg Television anchor revealed UUID information that disclosing UUID access would raise concerns among clients and terminal users. Hogan Lovells asked senior News management about the nature of the prohibition on disclosing journalist UUID access. While management said that no formal directive had been issued to journalists, management recognized that many journalists likely shared the view that disclosing UUID access would raise concerns among clients and terminal users.

Bloomberg Television anchor's on-air disclosure of UUID data. On September 15, 2011, reports broke in the global financial press that a major investment bank had suffered a large trading loss due to a rogue trader. Sometime prior to 7:30 a.m. (ET), Bloomberg Television had received sufficient confirmation of the trader's identity to name him on air. Other organizations did so as well.

A Bloomberg Television anchor was covering the story from the anchor desk and broadcast the following at approximately 7:29 a.m.:

We have been using the Bloomberg terminal, one of the unique tools that we have at our disposal, to find out a little bit about [the trader]. He is a Bloomberg user. Because he is a Bloomberg user, we know that the last login to this terminal yesterday at 2:00 in the morning, Eastern Time. Giving you an idea of the timeline of events today was the day that [the Bank] disclosed that it had the unauthorized trading losses. Using that as circumstantial evidence, we might conclude that [the Bank] did not know about this trading loss until very recently. Possibly as recently as yesterday.

The anchor told Hogan Lovells in interviews that he had not planned to use the terminal in his reporting nor had he discussed using the terminal with anyone. Rather, in working on the story, he recalled from his time in the newsroom that it was possible to access last login data through UUID. The anchor used a terminal on or adjacent to the set to look up the trader's UUID screen and immediately disclosed the login data on air.

In the interview, Hogan Lovells learned that the anchor was quickly approached by an editor and was subsequently admonished for disclosing UUID login data. He was told that the matter was being discussed by senior personnel within the organization. The anchor said he was surprised by this, as use of UUID data within the newsroom had never been an issue. He noted that he was not aware of anyone within Bloomberg Television having used UUID data prior to this telecast.²² The anchor said that over the next two days he had several conversations with senior personnel within Bloomberg Television and senior newsroom management. He understood that there was a concern that he had revealed confidential information on the air and that this was a serious issue. The anchor said that he has not used UUID for news purposes since that time.

The anchor's use of UUID data on air violated Bloomberg policy that prohibited the disclosure to third parties of confidential information. We find credible the anchor's statement to us that using the data was an extension of accepted newsroom practices with which he was familiar and that he did not recognize that UUID last login data was confidential. This, of course, does not excuse the violation but does provide context.

We also examined Bloomberg's response to the disclosure, which in our observation provided an opportunity for Bloomberg to terminate journalists' access to UUID screens other than their own. Hogan Lovells discussed this disclosure with some of Bloomberg's senior management. Based on the recollection of those individuals, it is clear that in the 48 hours immediately following the telecast there were multiple conversations amongst management. The issue attracted the attention of certain senior management, including Bloomberg's CEO, and various of these managers recall the CEO's directing that journalists' access to UUID should be turned off. Despite this, no such action was taken due to misunderstandings about who was responsible for doing so.

Journalist and BI Use of ADSKs

Although our testing did not reveal any instances where an ADSK view resulted in an Examined Article, it did not explain why journalists had accessed ADSK. We therefore, as discussed above, interviewed selected Newsmen about their ADSK usage. In addition, all Newsmen selected for interviews regarding UUID access were asked about ADSK as well.

²² From our review, it does not appear that UUID access by television reporters and anchors was frequent or pervasive. While many journalists were aware of and used this function, it appears that few if any television personnel did so. The differing backgrounds of the reporters and nature of their work help explain this difference.

Bloomberg employees interviewed. We identified the most frequent users of ADSK information as determined from the testing above. Some of these were Newspersons within the broadest definition, but had non-newsgathering functions (e.g., sales, circulation, or customer relationships) and were generally excluded from the analysis. Hogan Lovells interviewed the remaining Newspersons who frequently accessed ADSK and several individuals employed in BI who regularly accessed ADSK tickets. Hogan Lovells also asked Newspersons who were interviewed as part of the UUID review about ADSK usage. Because the nature of the work done by employees in BI was different from journalists, we separate our discussion of News and BI use of ADSKs.

Specific uses and frequency of ADSK access in the News division. Few Newspersons with whom Hogan Lovells spoke had ever accessed ADSK tickets. In fact, many of the Newspersons had never heard of ADSK, although they did recognize that terminal users could get assistance with technical or functional support from the Bloomberg Help Desk. Of the Newspersons who had accessed ADSK tickets, the following were identified as common reasons for this access:

- Direct responses to terminal users regarding specific articles. The vast majority of Newspersons who accessed ADSK tickets stated that the primary reason they did so was to respond to direct customer inquiries regarding articles the Newspersons had written. For example, Newspersons reported that readers would send ADSK inquiries about reporters' sources, to inquire more deeply on issues discussed in articles, or to request links to data underlying facts reported in articles. In those cases, reporters were either forwarded ADSK tickets or asked by Help Desk employees to provide information. In some cases, reporters would later access the ADSK entries to see how the issues were ultimately resolved or to follow up.
- Research regarding background of a source. Newspersons also reported reviewing users' ADSK tickets when they were preparing to speak to potential cited or anonymous sources for articles. By reviewing ADSK transcripts, journalists could glean information about the industry focus or other specialty of potential sources, which allowed journalists to determine whether particular terminal users were the appropriate individuals to approach about particular articles. In addition, Newspersons stated that they would review ADSK tickets to see if the terminal users had registered any complaints. Newspersons reported that this information would help them to establish a rapport with those individuals.
- Preparing for client visits. A smaller number of Newspersons, primarily located outside of the United States, reported using ADSK information in preparation for

sales visits to client offices. In some cases, journalists were asked to accompany terminal sales employees in order to explain how clients could better use terminal functions. Journalists also might attend sales visits to learn from clients about how Bloomberg News could provide better service or coverage to its readers. In preparation for these visits, some journalists would review ADSK tickets for the individuals with whom they were meeting so that they could familiarize themselves with the types of issues that the users had with the terminal.

In all of Hogan Lovells's interviews, Newspersons said they had not used ADSK information as a cited or anonymous source for articles. Several Newspersons stated that they did not understand how ADSK information could possibly be used for newsgathering. Some stated that they accessed ADSK tickets out of curiosity. With regard to each of the above-mentioned uses of ADSK information, we examined policies and procedures that were in place prior to April 19, 2013. These policies and procedures contained no specific or general prohibition of any of the uses that Newspersons reported in the interviews.

How journalists learned about ADSK access. Most Newspersons with whom Hogan Lovells met said they did not recall receiving specific training on the ADSK function. Newspersons stated that they likely learned about ADSK when terminal users raised questions through ADSK about news articles the Newspersons had written. One Newsperson stated that he or she learned about ADSK by simply exploring the terminal, and another Newsperson was aware that a user's ADSK tickets could be accessed through a link on the user's UUID page.

Transparency of use. In the interviews, Hogan Lovells asked Newspersons whether there had been any restrictions placed on their use of ADSK information or whether any concerns had been expressed at any level over the legitimacy or appropriateness of using such information. Of the limited number of Newspersons who accessed ADSK tickets, they reported that they were not aware of any attempt to restrict access to the ADSK function prior to the events of April of this year. Nor were they aware of any discussions about whether the use of the ADSK function by reporters was appropriate. However, a small number of Newspersons Hogan Lovells interviewed expressed discomfort at their ability to see ADSK tickets because of the free-form nature of ADSK requests.

BI employees' use of ADSK. In contrast to our conversations with Newspersons, employees of BI reported that they regularly accessed ADSK and often described ADSK access as an essential aspect of their jobs. BI is a separate division of Bloomberg unrelated to News, and BI employees are industry experts who provide data analysis and research in specific fields (e.g., oil and gas drilling). BI employees described themselves as "analysts,"

and although they engage in content generation for publications, they did not self-identify as journalists. The analysts acknowledged that they regularly provide brief written content on the Bloomberg “Dashboard.”

Specific uses and frequency of ADSK access in BI. Generally, the BI employees with whom Hogan Lovells spoke explained that they accessed ADSK tickets under three circumstances:

- First, they often were contacted by Help Desk employees when terminal users had questions about information in the BI employees’ respective industries of expertise. For example, an ADSK ticket regarding how to access certain oil inventory data would often be routed to a BI employee in the oil and gas team if the question could not be answered by the initial Help Desk employee.
- Second, higher-level BI employees stated that they would periodically search ADSK tickets for key words or technical terms that related to their industries in order to see whether the terminal users had been given the best answers to their questions. If a BI employee determined that there was better information available on the terminal in response to a terminal user’s question, the BI employee would send the user an email or message providing that information.
- Third, one higher-level BI employee Hogan Lovells interviewed stated that he would periodically review ADSK tickets from the last 90 days relating to his industry to see the types of issues in which customers were interested. The purpose of this review was to improve the overall Bloomberg product and to determine whether his team was focused on data and issues that were important to customers.

BI employees uniformly stated that they did not use specific client data from ADSK tickets in support of their research, analysis, or written product.

UUID and ADSK Access Findings and Recommendations

UUID Access

Findings. From the review described above, Promontory identified articles that Bloomberg published within two weeks following the UUID view and mentioned the terminal user or client associated with the UUID view (i.e., Examined Articles). In journalist interviews, Hogan Lovells asked Newspersons about the Examined Articles that related to their UUID views. We identified a small number of instances in which access to UUID data served as part of the newsgathering process for an article. With the exception of the anchor’s on-air disclosure, however, UUID data was not found to have served as a cited or anonymous source.

The ability of journalists to access UUID data about terminal users was well known within the newsroom by reporters, editors, and team leaders. A significant number of Newspersons, though far from all, accessed UUID data in the course of their work. We found that there was a widespread understanding among interviewees that UUID could not be used as a sole cited or anonymous source for reporting purposes.

Newspersons did not believe they were violating any policies or procedures in using UUID in their work. We found no indication, other than the anchor's disclosure of UUID data, that they were violating policies or procedures relating to client confidentiality or newsgathering. No Newsperson Hogan Lovells interviewed said that there was ever any discussion that use of such data without disclosure might violate the law or Bloomberg internal rules. However, several Newspersons stated that they were explicitly told or implicitly understood that UUID access should not be disclosed to terminal users.

Bloomberg News management failed to reexamine UUID access policies as the climate regarding customer privacy evolved.

Recommendations. To supplement Bloomberg actions already taken with regard to journalist access to UUID and ADSK, we recommend that the News division provide appropriate training and create formal plans for reexamining policies and key issues related to client privacy expectations. Regular examinations and training can assist in assuring that policies regarding both privacy and other issues in the newsroom keep pace with leading practices.

ADSK Access

Findings. From the review described above, Promontory did not identify any instances where it appeared that the ADSK information accessed by Newspersons led to the generation of an Examined Article. No Newspersons reported using ADSK information as a cited or anonymous source for an article.

The majority of Newspersons did not access ADSK, and many did not even know about the function. Those who did use ADSK stated that they primarily used it to respond to direct customer inquiries regarding their articles. In addition, journalists used ADSK in preparation for conversations with potential sources or visits with terminal clients. These uses did not violate Bloomberg policy or any external regulation.

BI employees regularly accessed ADSK as part of their customer service duties. Although BI employees viewed ADSK tickets for potential report topics, our review did not identify any

instances in which client-specific data from ADSKs was used as a basis for industry analysis or research.

Recommendations. We recommend that Bloomberg continue to restrict journalist access to ADSK tickets. Journalists should, however, be permitted to view and respond to ADSK inquiries related to articles they have written.

Additional Training and Other Actions

Bloomberg has reviewed our findings on the matter of journalist access to UUID and ADSK. In addition to steps already taken to change policy regarding journalist access to UUID and ADSK, Bloomberg has begun enhanced training for reporters and editors. Reporters and editors will receive mandatory training on client data policies and procedures. Editors will receive mandatory training on their responsibilities as managers. Furthermore, certain personnel will receive individual counseling on their responsibilities relating to the appropriate handling of Client Data.

B. Journalist Access to Other Functions Containing Client Data

Scope and Objectives

In addition to the review of UUID and ADSK access by Newsmen, we assessed other information that came to our attention during our review that related to Client Data accessed in newsgathering activities via terminal functions (other than UUID and ADSK) and presented the possibility of significantly impacting Bloomberg's clients or Bloomberg itself.

Methodology

Reports of potential access via other terminal functions came from a variety of sources. Some were presented to us by Mr. Hoyt following the interviews he conducted during his review of newsroom activities. Other reports surfaced through normal business channels, clients, public sources, or confidential sources. Regardless of the source, we assessed the credibility of all received reports. If a report was credible and within the scope of our work described above, we reviewed and analyzed it. Otherwise, we referred the report to Mr. Hoyt.

Our review of each credible report was tailored to the specifics of each report. Hogan Lovells conducted interviews and reviewed available materials. If appropriate, Promontory used both existing and purpose-designed testing to determine whether the claimed access existed. In most cases, the testing was tailored to the specific report of potential journalist access, for instance relating to the historical use of a particular function.

Specific Reports Regarding Access

We identified five reports that were deemed credible and required additional review. Each of these, and our findings with respect to each, is summarized below. In only one case did we find evidence of mishandling Client Data, and in that case, the journalist involved appears to have been unaware that the use was improper. In another case, we found that some journalists had access to a limited-access chat room under conditions that were not wholly transparent.

Access to Password-Protected Mortgage-Backed Instrument Data

We identified one instance in which journalists had access to information regarding a planned offering of a mortgage-backed instrument. That information was accessible to all Bloomberg employees, but non-employees required a password to access it. After viewing information about the instrument, a reporter published a short description of it.

By way of background, Bloomberg clients that wish to offer mortgage-backed or similar structured instruments (often referred to generally as “mortgage-backed instruments”) can place information about such instruments on the terminal. There is a terminal function that allows users to access such information. In some cases, the Bloomberg client (which is usually the issuer of the instrument, an underwriter, or placement agent) may desire to restrict access to the information posted on the terminal. To allow such clients to selectively share information about these instruments, Bloomberg offers a feature called Selective Security Access (“SSA”). This feature allows the terminal user supplying the information to set a password on the instrument. In such instances, the issuer, underwriter, or placement agent instructs Bloomberg to restrict access to information about the instrument, and Bloomberg marks the instrument as restricted. The default setting for an instrument marked as restricted is that access to information about the instrument will be controlled by a password; the issuer or underwriter assigns a password to the instrument and distributes the password to those terminal users with whom it wants to share the information. To indicate to terminal users that the instrument has been marked “restricted,” Bloomberg includes a purple shaded “S” on the screens that include information about that instrument. No terminal user, other than authorized Bloomberg personnel, can access information about the instrument unless the user has the password.

In December 2012, Bloomberg News published an approximately fifty-word description of a proposed offering of a mortgage-backed instrument that one of the lead underwriters had protected with a password. The reporter who wrote the description learned about the instrument by viewing the mortgage calendar function on the terminal. The instrument was

marked as restricted with the purple-shaded “S” symbol. Both the reporter and the editor associated with the article stated that they were not aware that the symbol indicated that information about the instrument was restricted and that such information was not available to all users of the terminal.

The lead underwriter for the instrument contacted Bloomberg on the same day the description was published. Bloomberg then reviewed the issue and determined that News should no longer have access to password-protected information about mortgage-backed instruments. Bloomberg terminated this access by changing the permissions afforded to Bloomberg News employees, so that News personnel’s access to information about password-protected mortgage-backed instruments is the same as that of all terminal users outside Bloomberg who have not received the passwords. Bloomberg implemented these changes by January 15, 2013.

During the course of our review, Bloomberg enhanced these technical controls to terminate access to password-protected mortgage-backed instruments for additional divisions within the company.

Findings. As part of the general review of access to Client Data, Promontory tested these controls and confirmed that employees within Bloomberg News and related divisions can no longer access information about those portions of mortgage-backed instruments that are marked as restricted and designated for password protection unless the employees receive the passwords, which are administered by clients.

During the course of our work, Bloomberg communicated to us its intention to terminate access to password-protected information about mortgage-backed instruments for divisions outside News that might publish content regarding those offerings. We endorsed that initiative and recommended that Bloomberg also terminate access to its Multimedia division. Bloomberg implemented those recommendations, and Promontory validated the effectiveness of the restrictions.

The December 2012 description of the mortgage-backed instrument should not have been published. The reporter and editor failed to recognize this due to the lack of proper training regarding the fact that the “S” symbol indicated that Bloomberg’s client did not want information about the instrument to be accessible to all terminal users. Additionally, Bloomberg’s lack of controls restricting journalist access to password-protected mortgage instruments was a clear deficiency.

Recommendations. Bloomberg should enhance its training program to help ensure that personnel understand the restrictions on access to and use of password-protected information regarding mortgage-backed instruments.

Access to Bloomberg Chat Room

We examined a report that reporters were participating in anonymous chat rooms without identifying themselves as such. We found evidence that journalists had access to the chat rooms and participated to some extent.

In 2011, Bloomberg created an anonymous chat room for certain commodities traders.²³ Permission to join and participate in the chat room was required prior to initial login and was obtained from the room's founder and moderator, an employee within Bloomberg's FX/Commodities group.

Starting in November 2011, the moderator approached several editors within the newsroom who worked in the commodities area and suggested that journalists working in the commodities field be given access to the room. Hogan Lovells interviewed a number of these editors. The moderator suggested to the editors that reporters could use the chat room to learn about the issues of interest to commodities traders, to follow current trends in real time, and to better react to user interests.

The Newspersons with whom Hogan Lovells spoke stated that, from the outset, the intention was that reporters would observe the chats but would not participate.²⁴ This, however, was not communicated in writing to anyone in the newsroom. Rather, each editor spoke to his or her own reporters, either in team meetings or as reporters were granted access to the chat room. At one point, reporters were told by editors to enter a code when joining the room that would prevent the reporters from posting comments. The editors with whom Hogan Lovells spoke stated that monitoring the room did provide a few ideas for articles and alerted them to articles that competitors were carrying. The chats themselves do not appear to have been used as source material, and there is no indication that reporters conducted interviews while using the anonymous feature of the room. Indeed, journalist activity on the site seems to have been limited to posting articles that had appeared elsewhere on the terminal without

²³ The moderator of the chat room, as administrator, was able to identify terminal users associated with posts. In addition, compliance personnel at terminal users' respective firms could identify terminal users; this was communicated to terminal users when signing into the chat room.

²⁴ The moderator did suggest to one Newsperson that the anonymous nature of the room would allow him to start discussions in the room. That reporter said that given instructions from his editor he did not do so nor did he know of anyone who did.

comment. Approximately 50 journalists had permission to access the room. Journalist access to this chat room was terminated in May of 2013.

There was no indication that users of the chat room were informed that journalists would have access to the room. At least two of the editors with whom Hogan Lovells spoke thought that the moderator may have mentioned in a post to the chat room that journalists could participate. We did not find any evidence of this post, but we did not examine records of all posts to the room.

Findings. Journalists' conduct in monitoring the chat rooms did not violate then-existing Bloomberg policy. Nor is there any indication that journalists intentionally misled terminal users about their participation in the chat rooms. Nevertheless, we believe that, given that the chat room was promoted to terminal users as a forum for traders, terminal users could have been unaware that chat room attendees could have included journalists.

Bloomberg revoked journalist access to the commodities chat room in May of 2013, and Bloomberg has taken steps to prevent journalist access to all anonymous Bloomberg chat rooms.

Recommendations. To the extent that Bloomberg decides to allow journalists to access anonymous Bloomberg chat rooms in the future, Bloomberg should explicitly notify terminal users that Bloomberg journalists may be viewing the chats and provide clear, written instructions to journalists regarding what constitutes acceptable conduct.

Access to Sales Database

Several sources raised concerns, which we conclude to be unfounded, that journalists were misusing access to a sales database. The sales database at issue is used by Bloomberg sales personnel to record information regarding prospects and terminal users, and to maintain records regarding sales contacts and conversations.

Journalist access to this database declined over time, with no more than six "front-line" news staff having access at any one time during the period from 2007 to 2013. No journalist has had access since May 1, 2013. We found no evidence that any journalist used the database as a source or lead for an article. One reporter did acknowledge looking in the database for a private cellphone number on one occasion.

We believe that the limited nature of journalist access in the past can be reasonably attributed to access provided to those journalists who participated in sales and commercial activities.

Findings. We found no evidence suggesting editorial use of information obtained by journalists via this sales database, and Promontory has verified that the database is not currently available to News personnel.

Visibility of Readership

We received reports that journalists could, even as of May of 2013, access information about what articles specific terminal users were reading. Based on Hogan Lovells's interviews and our examination of the terminal, we found these reports to be unfounded with one caveat. The terminal previously included a function that allowed all Bloomberg employees to view aggregate data about how many of a client's terminal users were reading particular articles. For example, the function could tell Bloomberg employees that 35 people at Bank X viewed article Y, but the function did not directly indicate who those 35 people were. For very small clients with one or two terminal users, the function provided unintended visibility into individual reading habits.

Findings. We did not find any evidence that any of the Newspersons with whom Hogan Lovells spoke used the function to bypass restrictions on viewing the reading habits of individual users. Moreover, Promontory's testing confirmed that no Bloomberg personnel have a privilege level permitting access to client usage data for this function. Bloomberg expressed that it will be retiring the function at issue.

This issue does, however, highlight the fact that given the complex nature of the terminal and its functions, careful consideration needs to be given to who is given access to what functions and whether the functions have unintended effects or abilities.

Access to Analysts' Ratings

Our review found no evidence that Bloomberg journalists had inappropriate access to analyst ratings reports. The Bloomberg terminal offers the ability to access ratings reports from analysts at many brokerage and investment firms. Some of the reports carried on the terminal have a restricted distribution that excludes Bloomberg journalists. Terminal users can access only those analyst reports for which they have viewing permission.

Bloomberg News, like many other organizations, has a group of reporters who focus on obtaining access to such reports and publishing articles about the reports promptly after their release.²⁵ The articles sometimes appear within minutes of the "official" release of a firm's reports to its clients. Given the prompt publication of these articles, several firms raised

²⁵ Indeed, there are websites that devote themselves solely to obtaining access to and publishing analyst reports.

concerns that Bloomberg journalists were using terminal access to obtain analyst reports for which they had no permission to view.

We reviewed these reports and concluded that they were unfounded. While we did not examine every news article regarding analyst reports, we viewed a sample of such articles and interviewed a number of reporters and editors who wrote these articles. We examined two possible scenarios. First, we considered whether reporters had terminal access to the reports. We saw no evidence that journalists had any access to analyst reports other than those for which they had permission. In some cases, certain investment advisors would allow broad access to their reports in order to generate publicity. Permissions were applied individually by administrators within each firm that chose to permit access.

We also considered whether it would be possible for a journalist to obtain hard or soft copies of such reports from Bloomberg's data operations without having terminal access to the published report. Strict safeguards exist that make this highly unlikely, and we saw no evidence of such actions. Rather, the Newspersons with whom Hogan Lovells spoke described a series of investigatory steps they undertook to obtain copies of the reports from individuals outside of Bloomberg who had authorized access.

Finding. We did not find any indication of improper access.

Additional Training and Other Personnel Actions

Bloomberg has reviewed our findings on these matters, including the issue of reporters monitoring anonymous chat rooms and the issue of a reporter and editor accessing password-protected data. Bloomberg has begun enhanced training for reporters and editors. Reporters and editors will receive mandatory training on Client Data policies and procedures. Editors will receive mandatory training on their responsibilities as managers. Furthermore, Bloomberg has committed to take appropriate personnel actions with respect to certain individuals involved in these matters.

C. The Message Posting

Background

As discussed above, the *FT* published an article on May 13, 2013 about the Message Posting. The article reported that a former Bloomberg employee posted the messages online while he was developing a product for Bloomberg. The article also reported that the messages were taken down from the website after the *FT* inquired about them. The *FT* article reported that the files posted online were "from one particular day in 2009 and also from 2010." Bloomberg obtained a copy of the file containing the 2009 messages from the

FT. The *FT* advised Bloomberg that it was unable to open the file containing documents from 2010. Through the work undertaken by WFG, Bloomberg was able to obtain from the former employee his copies of the message files posted online.

Prior to being posted online, the message files involved in the Message Posting were being used by Bloomberg, with client consent, to improve Bloomberg's "message-scraping" product – a product on which the former employee worked. A number of Bloomberg customers receive a large volume of messages containing price quotes in the course of using Bloomberg services. To make it easier to review pricing information quickly, clients and terminal users can elect to use Bloomberg-developed technology to parse the messages for security and pricing data. In order to allow the Quality Control group of the message-scraping team to further improve the product, Bloomberg asked certain buy-side traders to forward their messages to a designated Bloomberg inbox. The former employee later posted some of those messages online.

Scope and Objectives

Bloomberg initiated its own review of the Message Posting with the assistance of its counsel at WFG and Stroz Friedberg, an investigative and forensics firm retained by WFG. The objectives of Hogan Lovells and Promontory were to understand the nature of the Message Posting and confirm the appropriateness and thoroughness of the Bloomberg/WFG/Stroz Friedberg review.

Methodology

Hogan Lovells and Promontory consulted with WFG, Stroz Friedberg, and Bloomberg's legal staff as the review proceeded. Bloomberg, working with WFG, secured the former employee's cooperation during the review of the Message Posting. The former employee provided Bloomberg with his copy of the files that had been posted online.

We reviewed notes and memoranda prepared during the review. In addition:

- We consulted with Bloomberg's security team and individuals who work with the message-scraping product;
- WFG interviewed the former employee on June 5, 2013, and provided Hogan Lovells with a detailed briefing from that interview. WFG also conducted numerous follow-up discussions with counsel for the former employee. WFG briefed Hogan Lovells on those discussions;
- WFG and Stroz Friedberg analyzed the logs of the websites registered to the former employee to determine how often the material online was reviewed or

accessed. WFG and Stroz Friedberg performed searches to determine whether the message files were available elsewhere on the Internet and determined that there was no information to suggest that the message files remained available on the Internet;

- With the former employee's consent, WFG retrieved from the former employee numerous files and computing devices received access to the former employee's personal email accounts. WFG and Stroz Friedberg reviewed those materials for information that belonged to Bloomberg or Bloomberg's clients and briefed Hogan Lovells and Promontory on the materials recovered; and
- Promontory assisted Bloomberg in reviewing certain message files received from the former employee to determine which client messages were posted online.

Findings

Nature of the Files

Bloomberg determined that the former employee had improperly posted three message files:

- One containing messages from August 28, 2009 (the file viewed by the *FT*);
- One containing messages from September 10, 2010; and
- One containing messages from September 6-10, 2010.

WFG's review, including the review of the logs of the former employee's websites and analysis of the other devices, files, and email accounts recovered from the former employee, did not uncover any evidence that the former employee improperly posted online any other Client Data that the former employee accessed through his employment at Bloomberg.

The files posted online consisted of messages that had been forwarded to Bloomberg's inbox by buy-side traders from various firms.

A Bloomberg client's or terminal user's messages could have been included in the messages posted by the former employee in one or more of the following ways:

- If the client or terminal user forwarded messages to the Bloomberg inbox for use in improving the message-scraping product;
- If the client or terminal user sent a message to another user who forwarded messages to the Bloomberg inbox; or

- If the client or terminal user received or sent a message that was concurrently or subsequently sent to another terminal user who forwarded messages to the Bloomberg inbox.

Bloomberg reviewed the files to determine which clients had been affected by the Message Posting.

The Former Employee's Reasons for Posting the Files

According to the former employee, he posted the message files online for two reasons:

- He wanted to be able to analyze the messages outside of the development environment in a manner that exceeded his permitted abilities on Bloomberg systems; and
- He wanted to convince Bloomberg's senior management of the viability of his ideas for further developments to the message-scraping product.

Bloomberg's Notification to Its Customers

Bloomberg employees reviewed the files received from the *FT* and from the former employee for the limited purpose of determining which of its clients whose terminal users had forwarded messages to the Bloomberg inbox had messages posted by the former employee. Bloomberg voluntarily notified each of those clients about the posting. For each client that so requested, Bloomberg also provided a copy of the messages involving the client that had been posted online.

For clients whose terminal users had not forwarded messages to the Bloomberg inbox and who asked Bloomberg about whether their messages were posted online, Bloomberg searched the message files to determine whether any of those clients' messages were posted. Those clients' messages could have been posted if the clients sent messages to a terminal user who forwarded his or her messages to Bloomberg's inbox or if the clients were co-recipients of messages sent to such a terminal user. As with the clients whose terminal users forwarded messages, Bloomberg provided a copy of the client's messages to any client that so requested.

As noted, the former employee involved in this matter cooperated with Bloomberg in its investigation. Bloomberg has reserved its rights with respect to any legal steps it may take with respect to that former employee.

Bloomberg's Controls

In posting the files, the former employee violated Bloomberg's policies prohibiting such actions.

Prior to the discovery of the Message Posting and prior to our engagement, Bloomberg had already enhanced the controls to monitor and help prevent data transfers outside its systems, including the message-scraping environments.

Additional information about the current state of Bloomberg's message-scraping controls can be found in Section 7.

6. REVIEW OF CLIENT RESPONSES AND PUBLIC STATEMENTS

A. Objectives and Scope

Promontory and Hogan Lovells assessed the accuracy of Bloomberg's public statements and Bloomberg's written communications to clients about its Client Data practices that were issued soon before or during our engagement. These statements and communications included public comments of Bloomberg executives, general update letters to clients, and specific responses to individual client inquiries ("individual communications") (jointly "Client Communications"). Bloomberg issued ten public/general statements in the timeframe covered by our review.

B. Methodology

The review of Bloomberg's client statements included the following steps:

- Obtaining the relevant Client Communications issued prior to our engagement;
- Reviewing the Client Communications for statements about Bloomberg's current or past practices or controls relating to Client Data ("assertions");
- Evaluating assertions against available evidence;
- Working with Bloomberg during the course of our engagement to construct a framework for preparing appropriate public statements and communications to clients, including, in many instances, drafting assistance (provided by Hogan Lovells) and evaluating assertions against available evidence prior to release (provided by Promontory); and
- Considering whether Bloomberg issued accurate updates to clients when new information warranted updating previous statements, and evaluating Bloomberg's updates against available evidence.

Public Statements and General Statements Reviewed

Hogan Lovells and Promontory reviewed all of the public statements and general updates released by Bloomberg between May and July 2013.

Individual Communications Reviewed

Promontory reviewed all individual written communications.

Selecting Assertions for Review

The principal criteria for selecting assertions were whether their accuracy would likely be of importance to clients and whether they were verifiable. Subjective statements (e.g., “We are deeply committed to safeguarding the integrity and confidentiality of our clients' data in all situations and at all times”) were generally not selected but more-detailed statements were (e.g., “[Our reporters] had access to . . . a terminal user's login history and when a login was created . . .”).

Evaluating Statements Against Available Evidence

Each selected statement was assessed for accuracy against available evidence. For Client Communications issued during our engagement, Promontory tested many proposed assertions against available evidence prior to Bloomberg issuing them. Other assertions were tested after issuance against available evidence. The available evidence included Bloomberg documentation, the known results of the ongoing Promontory testing, and the results of discussions and interviews with Bloomberg staff. Each statement was then classified as to the degree it was supported by evidence.

C. Findings and Recommendation

Promontory's testing confirmed that the factual statements in Bloomberg's Client Communications were accurate in all material respects.

For instance, Promontory's testing confirmed the accuracy of Bloomberg's statements that Client Data relating to trading activities, messaging, or portfolio information were not available to journalists and were protected by security measures appropriate to their sensitivity. Promontory also confirmed, after initial testing revealed the need to expand the scope of the permissioning changes to cover Bloomberg journalists who work outside of the core news function, that Bloomberg had successfully implemented its announced policy of restricting journalist access to UUID and ADSK.

Hogan Lovells and Promontory's review also found that Bloomberg issued accurate updates to clients as it received new information from the outside review it commissioned concerning the Message Posting. Bloomberg promptly notified affected clients of the discovery of additional posted files.

Promontory's testing of Bloomberg's statements identified one assertion that contained a minor and immaterial inaccuracy:

- A statement said, “Our employee confidentiality agreement and company policies explicitly prohibit disclosure of confidential information. Employees are reminded

of this obligation by way of periodic email notifications.” The description of the prohibition is accurate, and there are periodic email notifications regarding a range of policy and governance issues. For example, an email notification sent on April 11, 2013 stated, “Since confidentiality cannot be assured when using the Internet or e-mail, you may not upload Company documents or confidential or proprietary information to a non-Bloomberg email address.” However, the email notifications reviewed did not include mention of the prohibition on disclosing confidential information.

Considering the nature of this inaccuracy and the disclosure of the nature of this inaccuracy in this Report, we are comfortable that the inaccuracy did not merit additional communications to clients to correct the statement prior to the issuance of this Report.

We have recommended that Bloomberg adopt a more-regular practice of reminding its employees of their Client Data confidentiality obligations.

7. REVIEW OF CURRENT CLIENT DATA POLICIES AND PRACTICES

A. Objectives and Scope

As explained in the Introduction, our mandate included reviewing the current state of Client Data policies and procedures at Bloomberg and Bloomberg's proposed future changes to them.

We assessed the Client Data compliance framework as of the date of this Report, including:

- Tone at the top;
- Governance;
- Internal controls, including policies and procedures, in terms of their design, content, and implementation;
- Ongoing employee training; and
- Accountability mechanisms.

We also assessed Bloomberg's plan to enhance its framework and controls going forward, including its prospective testing methodology.

We assessed the current Client Data compliance framework against:

- Accepted international standards, including:
 - ISO 27000, used by many organizations with multinational operations because of its broad, globally-minded approach to the development, implementation, and improvement of information security management systems;²⁶
 - COBIT, published by ISACA,²⁷ which integrates themes from several other major standards, including ISO 27000; specifically discusses the role and governance of information technology from an enterprise-wide perspective; emphasizes regulatory compliance; and helps organizations align the goals, benefits, and risks of information technology with the goals, benefits, and risks of the enterprise;²⁸
 - NIST 800-53, published by an agency of the U.S. Department of Commerce and directed toward U.S. federal agencies and companies that do business

²⁶ <http://www.itgovernance.co.uk/iso27000-family.aspx>.

²⁷ Formerly known as the Information Systems Audit and Control Association.

²⁸ <http://www.isaca.org/COBIT/Pages/default.aspx>.

with the U.S. government and “process, store, or transmit [U.S.] federal information.”²⁹ Many non-U.S. government organizations follow NIST 800-53 because it maps to ISO 27000 very closely and offers specific, quantifiable actions that organizations should take with respect to information security;³⁰

- ITIL, published by the UK government and often used by organizations that are based or that operate in whole or in part outside of the United States;³¹ and
- Fair Information Practice Principles (“FIPPs”) for handling data relating to individuals, as expressed by various governmental organizations such as the OECD.³²
- Expectations for vendors working with regulated financial institutions, such as those expectations contained in the FFIEC’s Information Security Handbook; and
- Industry-leading practices, including:
 - Implementing a documented and auditable change management program;
 - Segregating production and development environments, with non-public data relating to clients limited to production;
 - Regular information security training and awareness programs throughout the enterprise;
 - Appropriate governance and oversight of information security program activities;
 - Alignment of the IT risk-management program with strategic goals;
 - Regular independent reviews and audits;
 - Robust vendor risk-management program;
 - Well-documented control processes with corresponding written procedures; and
 - Comprehensive and regular monitoring of vulnerabilities and security risks.

²⁹ http://www.nist.org/nist_plugins/content/content.php?content.18.

³⁰ <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.

³¹ <http://www.iti-officialsite.com/WhatIsITIL.aspx>.

³² *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Part Two-Basic Principles of National Application*, OECD, <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>; *Fair Information Practice Principles*, FTC, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>.

We reviewed Bloomberg's management of Client Data across the whole organization, including Bloomberg's regulated financial entities. We applied the same assessment criteria where Client Data was processed by those regulated entities as we did elsewhere. We did not undertake a separate regulatory review of the regulated entities.

B. Assessment of Overall Client Data Compliance Framework

Tone at the Top

Standards. The tone at the top should emphasize the importance of risk management in general and the appropriate protection and use of Client Data in particular. There should be regular, ongoing, and clear communications from management regarding the importance of handling Client Data appropriately. These communications should address both the spirit of the principles in place and the importance of adhering to the policies and procedures supporting those principles. The actions of senior management should reflect and reinforce their communications. The tone at the top should cascade from the senior executives through other layers of management. The tone at the top should be effective as judged by the words and actions of individual employees at all levels.

Findings. From the start of our work in May 2013, we observed that Bloomberg's Chairman, Bloomberg's CEO, and other senior executives issued clear, repeated communications to Bloomberg personnel regarding the importance of complying with controls to protect the confidentiality of Client Data. These communications have included emails and public blog postings, directives to adopt Client Data policies and procedures, and an upcoming "Town Hall" meeting³³ that will further address these themes. We have seen the same themes reiterated informally by senior management in their interactions with staff and with us during the course of our work.

These communications carried with them an appropriate sense of urgency to enhance the current state of Bloomberg's controls and a commitment to continuous self-improvement.

These communications have been reinforced by the actions taken by senior management, including:

- Providing transparent and specific responses to client inquiries about Client Data policies and practices, particularly around data access controls and the results of testing of those controls;

³³ We reviewed a script of remarks to be delivered at this Town Hall meeting.

- Adopting, at the level of the Board of Directors, Bloomberg's Client Data Principles governing protections of, access to, and use of Client Data (these Client Data Principles are attached as Appendix F);
- Approving policies to formally document and enhance existing practices;
- Direct and ongoing involvement by senior executives in the design and implementation of control enhancements, such as the "Walled Garden"—a segregated environment containing restricted data to which Bloomberg personnel are granted access on a controlled basis when a development project requires use of such data; and
- Day-to-day actions that reinforce the importance of appropriate controls (e.g., in a practice that compares favorably to what we have observed at many regulated financial institutions, Bloomberg's senior executives wear security badges at all times and badge in and out of Bloomberg offices).

In our review, we found evidence that managers at various levels reiterate or "cascade" this tone at the top at staff meetings, in communications to staff, and through actions such as resource allocation. Further, in the course of our review, we interviewed over 200 employees and interacted with many more as we gained information about Bloomberg and its controls. In many of these interviews and interactions, we found that Bloomberg employees had received and incorporated the messages being communicated from the top and reiterated at various layers of management.

Based on interviews and documentation reviewed, we also found that prior to the events of Spring 2013, there was some messaging that characterized control processes and infrastructure as noncritical bureaucracy, and our review found some vestiges of that messaging.

Recommendations. Opportunities to enhance the tone at the top include:

- Continuing to cascade the tone at the top established by senior executives and supporting Bloomberg's efforts to enhance its culture around risk and compliance. This is particularly important in the news businesses, where the tone at the top has not always been communicated as effectively as it could have been.
- Maintaining Bloomberg's respectful attitude toward risk and compliance professionals and the need for a strong internal audit function.

Governance

Standards. Governance should provide effective oversight, clear allocation of responsibilities, and efficient channels for escalating and resolving actual or potential control weaknesses. Key governance standards of particular relevance to Bloomberg are summarized below.

Management Responsibilities. In well-governed organizations, management owns risk and serves as the first line of defense in managing risk within tolerances established by senior management and the board of directors. In many organizations, there is typically a risk management committee comprised of senior executives to manage risk on a cross-functional basis.

Board Responsibilities. Unlike private companies such as Bloomberg, oversight at public companies is performed by a board of directors with fiduciary responsibilities to public shareholders. Typically, board oversight at public companies includes dedicated committees comprised of a majority of independent directors with oversight responsibility for particular control functions such as audit and risk. As a private company, Bloomberg is not subject to the same expectations. However, many private companies have adopted board-like mechanisms to enhance governance.

Board Audit Responsibilities. At public companies and private companies that choose to adopt similar standards, boards are responsible for establishing effective, independent audit functions. In addition to hiring external auditors, the leading practice is to not completely outsource internal audit activities and to retain board responsibility where audit activities are outsourced.

The Role of Internal Audit. The audit function should be accountable to the board. The audit function should provide independent assurance to the board and senior management on the “quality and effectiveness of . . . internal control, risk management and governance systems and processes, thereby helping the board and senior management protect their organization and its reputation.”³⁴ An effective internal audit function should have the following characteristics:

- Independence;
- Sufficient and qualified resources;
- Comprehensive scope;

³⁴ Basel Committee on Banking Supervision, *The Internal Audit Function in Banks* (2012); see also Institute of Internal Auditors, *International Standards for the Professional Practice of Internal Auditing (Standards)* (Rev. 2012).

- A risk-based audit planning process;
- Compliance with sound internal auditing standards and ethics; and
- Quality assurance.

Last and most important, an effective internal audit function should identify the issues, problems, and opportunities for enhancement that all complex, dynamic organizations have. The best-governed organizations use internal audit, as well as other mechanisms, to find them.

Risk and Compliance. Many organizations include a risk and compliance function as part of their governance framework. This is true not only of financial institutions, where such functions are required, but also of many non-financial companies, particularly those that face significant operational or compliance risks. Risk and compliance functions should be independent of line-of-business management. They often report to the chief executive and should have the ability to provide information directly to the board of directors. They should also have sufficient stature, authority, resources, and access to information to be effective. In a well-governed organization, the risk and compliance function serves as a second line of defense, between line-of-business management and the internal audit function.

Findings. With respect to management's role in governance, we found Bloomberg to have a management team that was closely focused on the issues relating to Client Data policies and practices, including a management committee comprised of the most senior executives at Bloomberg that met regularly, set direction, approved principles and important policies, and received updates on program status.

Bloomberg has a Board of Directors comprised of six senior executives and three independent directors. The Board recently changed the title of its Audit Committee to "Audit, Risk & Compliance Committee;" expanded the committee's mandate; and changed the composition of the committee so that it now has a majority of independent directors. Hogan Lovells³⁵ found that the current independent directors, considered together, bring extensive experience in financial services, governance at financial and non-financial companies, financial controls, and risk management, including regulatory expectations of information security and privacy controls at financial institutions and their vendors. The Board has adopted a charter for the Committee that, among other things, establishes the Board as

³⁵ Because one of the independent directors of Bloomberg, Inc. (the General Partner of Bloomberg) also serves as an Advisory Board member to Promontory, this finding and the related recommendations are those of Hogan Lovells, rather than a combined finding of Hogan Lovells and Promontory.

accountable for an effective internal audit function. Bloomberg has approved plans to establish independent internal audit and risk and compliance functions that meet the standards described above.

In terms of standards governing Bloomberg's handling of Client Data, Bloomberg's Board of Directors has approved a set of Client Data Principles (attached as Appendix F), and Bloomberg's management committee has approved the following policies:

- Information Security Policy;
- Client Data Classification Policy;
- Access Control Policy; and
- Personal Client Data Privacy Policy.

Other policies are approved by a Policy Approval Committee whose members are senior managers not heavily involved in the day-to-day management of Client Data.

In addition, we found the following relevant elements of governance at Bloomberg:

- The Board of Directors commissioned independent advice from Mr. Palmisano;
- Management appointed a senior executive with temporary overall project-management responsibility for coordinating Bloomberg's rapid response effort to assess and improve its controls;
- Management created a cross-business-unit working group to support the executive mentioned in the previous bullet;
- Management has established the position of Chief Risk and Compliance Officer with a reporting line independent of line-of-business management³⁶ to play a key role in managing Bloomberg's risk and compliance program, including controls;³⁷
- Management has appointed a Client Data Compliance Officer who is independent of line-of-business management,³⁸ oversees controls around the protection and use of Client Data, and is supported by resources to manage improvements to those controls (as well as a commitment and plan that is currently underway to expand those resources);

³⁶ The reporting line will be direct to the CEO and indirect to the Chairman of the Board.

³⁷ Bloomberg has created a position description for this role, with input from Hogan Lovells and Promontory, and is recruiting to fill it.

³⁸ The Client Data Compliance Officer reports directly to the CEO. After the Chief Risk and Compliance Officer position is filled, the Client Data Compliance Officer will report to the Chief Risk and Compliance Officer.

- Bloomberg has a Head of Security³⁹ whose reporting line is independent of line-of-business management and supported by resources to support additional testing of controls and other measures;
- Management has committed to expanding and formalizing the internal audit function to audit compliance with Client Data policies, procedures, and other controls; and
- Bloomberg has escalation channels, including anonymous hotlines for employees to use to report breaches or concerns.

We note that Bloomberg's Client Data Compliance Office ("CDCO") Program is currently an effective change management program that has tightened a number of access restrictions and implemented many control enhancements. The Program has also begun to institute a range of "business as usual" measures, such as developing a network of access administrators within the business and formalizing a number of procedures. However, the CDCO Program is not yet fully staffed or fully embedded into Bloomberg's ordinary business operations. Given the high volume of change planned in forthcoming months, as evidenced in the CDCO Roadmap (discussed below), the focus of the CDCO Program on change management remains appropriate. However, once Bloomberg hires a Chief Risk and Compliance Officer, Bloomberg should give more consideration to the long-term relationship between the CDCO Program and the Risk and Compliance function.

We also note that Bloomberg's approach to governance includes periodically commissioning third parties to advise on potential enhancements to its information security and privacy controls. However, Bloomberg did not always effectively log third-party recommendations, track their implementation, or document Bloomberg's considered rationales for rejecting or deferring implementation of recommendations. Some of the recommendations that Bloomberg received prior to our engagement, such as enhancing Bloomberg's compliance risk-management infrastructure and segregating the development and production environments, might have, if implemented, anticipated recommendations that arose from our review.

Recommendations. Opportunities to further enhance governance include:

- Ensuring that the Audit, Risk & Compliance Committee continues to be comprised of a majority of independent directors;

³⁹ Currently, the Head of Security reports to the Chairman of the Board. After the Chief Risk and Compliance Officer position is filled, the Head of Security will report to the Chief Risk and Compliance Officer.

- Periodically assessing the effectiveness and mandate of the Audit, Risk & Compliance Committee. Some organizations find that the agenda of a single committee becomes too full to allow the committee to effectively oversee audit, risk, and compliance. This periodic assessment should also determine whether the members of the Audit, Risk & Compliance Committee have the time, requisite experience, and resources necessary to make the Committee effective;
- Filling the newly created position of Chief Risk and Compliance Officer with a qualified person and providing the position with an adequate staff and budget, sufficient stature and authority within the organization, and access to data and other resources needed to assess the state of Client Data controls;
- Developing a migration plan to transform the CDCO from a change function into a “business as usual” division;
- Completing the implementation of the governance-related components of the Information Security Policy, particularly the information security risk assessment. This risk assessment should build on the testing performed in the course of our review. Bloomberg should use the results of the risk assessment to further enhance its information security risk-management program;
- Establishing and staffing an independent, internal audit function with appropriate resources in terms of both quantity and qualifications;
- Charging the Audit, Risk & Compliance Committee with the task of validating that the approved recommendations of this Report have been implemented fully; and
- Implementing better mechanisms for tracking and following up on recommendations from external and internal sources, including implementation of the recommendations from this Report.

Internal Controls

This section is comprised of two parts: a) our review of Bloomberg’s Client Data policies and procedures and b) our assessment of the design and implementation of the key controls that implement those policies and procedures.

Policy and Procedure Design and Content

Standards. Policies and procedures should:

- Align with the statement of principles endorsed by management (in Bloomberg’s case, the Client Data Principles);

- Reflect applicable law, accepted international standards, and industry-leading practice;
- Be clear on the allocation of responsibilities to different parts of the business, including identifying the overall owner of each policy or procedure;
- Be written in a simple, direct, and actionable manner so that they are unambiguous and easily understood;⁴⁰ and
- Be subject to periodic (at least annual) review to help ensure that they:
 - Remain consistent with the organization's operations and risk profile; and
 - Are updated to reflect changes in legal and regulatory requirements, relevant standards, and industry-leading practice.

Findings. Bloomberg has developed a hierarchy of principles, policies, and procedures to govern its handling of Client Data.

- Client Data Principles (reproduced below in Figure 1 and as Appendix F). This is a document that articulates the principles by which Bloomberg intends to handle Client Data.
- Client Data Policies (listed below in Table 1). These eleven policies describe Bloomberg's standards for compliance with the Client Data Principles, accepted international standards, applicable law, and industry leading practices. The policies also assign roles and responsibilities for meeting the standards and establish consequences for non-compliance. They provide for periodic (at least annual) review and updating. The policies follow a standard format and refer to a common glossary of defined terms.

While these policies have been adopted recently as formal, documented policies, most of them formalize policies and practices that were largely in existence prior to our engagement. The exceptions are Bloomberg's Access Control Policy, which reflects recent enhancements to Bloomberg's approach to permissioning employee access to data, and the Vendor Management Policy, which reflects an expansion of vendor management from a process that was focused on due diligence at procurement to a more formal, risk-based program for the selection, contracting, and ongoing oversight of vendors.

⁴⁰ Policies and procedures should be drafted in a standardized format wherever possible to support easy comprehension and a consistent approach.

We are of the view that the eleven Client Data policies adequately address the issues they are intended to cover and provide a sound basis for managing the risks to Client Data in their respective areas.⁴¹

- Client Data Procedures. These procedures describe how Bloomberg will implement the standards described in the Client Data policies. Bloomberg has a number of procedures in place. It has completed the documentation of additional high-priority procedures and has a plan to complete the documentation of additional remaining procedures in the next six months.

We are of the view that the completed procedures adequately address the issues they are intended to cover and provide a sound basis for managing the risks to Client Data in their respective areas.⁴² We have also reviewed the schedule for completing the remaining procedures. We found that the most critical procedures have been implemented and that the schedule and prioritization of the remaining procedures is reasonable.

Recommendations. Opportunities to further improve the design and content of Bloomberg's Client Data policies and procedures include:

- Finalizing the procedures required to support its Client Data policies;
- Completing Bloomberg's plan to provide personnel with a tailored set of policies and procedures relevant to workforce roles and available via the terminal; and
- Staggering the review of the recently formalized policies and procedures to spread the review work across the year (this will require reviewing some of the recently formalized policies before their one-year anniversary date).

⁴¹ Hogan Lovells and Promontory advised and assisted Bloomberg in drafting the Client Data policies.

⁴² Hogan Lovells and Promontory advised and assisted Bloomberg in drafting procedures.

CLIENT DATA PRINCIPLES

Bloomberg clients rely on our unique financial solutions and exceptional customer service. These solutions and services require the thoughtful integration and analysis of client, third-party and proprietary Bloomberg information. Client trust is therefore our highest priority and the cornerstone of our business.

These Client Data Principles inform and guide decisions made throughout Bloomberg by our employees, contractors, and temporary staff (collectively, "Personnel") about data we collect from our clients and end users through their use of Bloomberg's products and services ("Client Data").

Respect: We handle Client Data in a manner respectful to our clients and end users. We constantly examine how our principles, policies and procedures help us provide the protection our clients deserve and we respond thoughtfully to their questions, opinions, and concerns.

Transparency: We communicate with clients about our policies for Client Data. Accurate and useful information about our Client Data practices is available through our products and services, Bloomberg.com, customer service, and other authoritative sources.

Personnel Access: We grant Personnel access to Client Data only as necessary for them to carry out their responsibilities. Such access is regularly reviewed and confirmed through our role based permissioning systems and procedures.

Security and Privacy: We invest in and maintain administrative, technical, and physical safeguards to protect Client Data. We engage in ongoing monitoring and testing of the efficacy of these safeguards.

Innovation: We constantly seek to create value for our clients through innovation, and we apply the same approach to our Client Data practices. By referencing relevant international security and privacy standards and building new solutions that anticipate the unique needs and concerns of our financial services, government and corporate clients, we establish industry-leading practices.

Personal Accountability: All Bloomberg Personnel are personally accountable for acting consistently with these Principles and in accordance with relevant policies and procedures. We understand that there are consequences for behavior that is inconsistent with these Principles.

Governance: Senior management is responsible for strong and effective governance, including ensuring that we implement the letter and spirit of these Principles through policies, procedures, training, monitoring, testing, and auditing.

Figure 1

Table 1 Bloomberg Policies for Client Data	
Policy Name	Description
Client Data Classification	Classifies Client Data by category and defines the roles that can access that data.
Access Control	Defines the rules and processes for granting personnel access to Bloomberg applications.
Information Security	Explains the security organization, roles and responsibilities, and requirements (e.g., monitoring, audit, and testing requirements) for security operations, risk assessment, vulnerability management, asset management, disaster recovery, and systems development life cycle.
Personal Client Data Privacy	Addresses additional requirements for handling personally identifiable information within the scope of Client Data.
Vendor Management	Defines requirements, roles and responsibilities, and authority for the selection, contracting, and ongoing oversight of third-party vendors.
Personnel Management	Specifies the management of operational risk in connection with hiring (e.g., background screening), training, discipline, termination of access, and return of assets.
Incident Response	Describes the process for responding to incidents (e.g., security breaches).
Physical Security	Mandates the safety and security of facilities and employees, and describes the controls to enable these goals.
Business Continuity	Defines the business requirements, roles and responsibilities, and processes (e.g., business impact analysis, plan development and maintenance, and testing) for ensuring system and data availability, recovery, and resiliency.
Records Retention Policy	Prescribes standards for the retention and management of Bloomberg's records.
Global Resource and Information Core Guide & Contingent Worker Policy Guide	Defines conduct standards for Employees and Contingent Workers.

Implementation of Key Controls

Data classification, encryption, and retention

Standards.⁴³ ISO 27002 Section 7.2, part of the ISO 27000 series, requires that information be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization; that the classifications be formally evaluated on an annual basis; and that the classifications be documented as part of an IT Risk Assessment. A formally documented data classification policy should be issued and enforced through the use of technical controls throughout the network, applications, and databases. Certain types of data should be encrypted whenever they are transmitted outside of the network.

An overarching data retention policy should be in place to define the proper retention period for each class of data. This requirement is contained within COBIT Section PO2.3-Data Classification Scheme. The retention program should include a process to purge data when it is no longer needed, as well as a process to retain data past its defined retention date when business or legal needs arise.

Findings. We found data classification and encryption controls to be appropriately designed and implemented. We found data retention controls to be appropriately designed and that recent enhancements to those controls are being implemented.

Bloomberg's current Client Data Classification Policy was approved during the assessment period; however, the concept of restricting access to certain classes of Client Data existed at Bloomberg prior to our engagement. In light of recent events, Bloomberg recently performed significant work to evaluate the data classification and access restriction processes in place, and the implementation of the Client Data Classification Policy is firm wide. We noted that the recently released Client Data Classification Policy addresses categories of Client Data but does not include definitions or handling procedures for other categories of data, such as employee data or proprietary data.

Access to data over the Internet is protected using SSL encryption. There are additional tools in place to encrypt data traveling outside of the organization, including secure FTP for file transfers. Bloomberg's data retention procedures are currently being aligned to Bloomberg's Records Retention Policy.

⁴³ In this "Implementation of Key Controls" section, the Standards sections summarize key standards of particular relevance to Bloomberg for each of the key controls we reviewed.

Recommendations. Opportunities to further improve data classification, encryption, and retention include:

- Completing the data retention procedures that support the Records Retention Policy;
- Implementing technical controls and allocating additional resources for CDCO and Legal to enforce applicable data end-of-life procedures in accordance with the Record Retention Policy (and the supporting data retention procedures when they are completed); and
- Expanding the Client Data Classification Policy to include additional data types, such as employee and proprietary data.

*Change management/Systems Development
Life Cycle (“SDLC”)*

Standards. Change management in this context encompasses software patch management, system development, and release management. Both COBIT Section PO6 and ISO 27002 Section 12.5 provide relevant frameworks for large organizations to manage change and systems development. Organizations should have change management policies and procedures in place to help ensure that changes intended for production environments are authorized, coordinated, and controlled so that changes have minimal impact on the production environments. Processes and procedures for implementing change may be universal for the organization (i.e., applicable to all business lines and environments) or may be stratified (e.g., differentiating between changes affecting the entire organization and those affecting a particular business line, product group, support area, or affiliate). Organizations may choose to develop individualized procedures for specific hardware architectures or applications.

Findings. We found change management and SDLC controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

The IT environment at Bloomberg is dynamic, and urgent change requests requiring rapid deployment are common. Currently, R&D resources can use production data to support testing and be granted access to production to make emergency fixes within the production environment. This activity is currently logged but is not proactively monitored. We observed a series of product-specific processes and procedures designed to mitigate the risks associated with software design and implementation. Development of new application functionality follows a variety of methodologies and is tracked using multiple in-house-developed internal ticketing systems. Our assessment included a review of both large and

small development projects spanning ten product areas and walk-through testing. We accomplished this by sitting with development resources and observing tracking tickets for the various projects from inception to release. Irrespective of the various development methodologies used, overarching security reviews embedded in the design, testing, and deployment process sufficiently mitigate the overall risk related to change management and SDLC.

We noted instances in which production data is used in the development and testing environments without being obfuscated or scrubbed. Additionally, there is not currently a process to remove the production data from the development and testing environments when it is no longer needed.

Recommendations. Opportunities to further improve change management and SDLC controls include:

- Developing a plan to enhance the segregation controls between development, test, and production environments;
- Enhancing its development and testing environments to more closely mirror its production environment;
- Consolidating the systems for tracking changes to software code;
- Documenting the change management and SDLC processes to provide clarity and consistent application of authorized approaches and to determine whether the appropriate groups are engaged throughout the process;
- Regularly reviewing and auditing production access ticketing systems for policy compliance; and
- Monitoring production activity logs for irregular or inappropriate activity.

Application security

Standards. Large organizations should control access to applications by using authentication and authorization controls commensurate with the risks associated with the applications. Logical access rights should be monitored to determine whether they are assigned based on the minimum requirements for users' current business needs. Effective application access control involves a partnership among security administrators, application developers, and business owners. Controls should also be in place to support the logging of access and security events and the proactive analysis of user activities in order to preserve the integrity, availability, and confidentiality of application data.

Findings. Bloomberg applications run within their own proprietary infrastructure, which allows for centralized identity and access management. Bloomberg has adopted and implemented a role-based permissioning (“RBP”) system as a means to enforce individual access to data systematically. RBP leverages the existing privileging function (“PVF”), which is designed to restrict employee access to defined Client Data types based on the enterprise Client Data classification standard. Through RBP, Bloomberg is able to limit access to those personnel who have a “need to know” the data consistent with their job responsibilities. The granting of administrative access and modification of roles and access to different classes of data are managed by the CDCO. We noted that logs of user activity are maintained but currently are not monitored or reviewed proactively for suspicious or inappropriate activity.

Our testing initially indicated that some functions protected by PVF levels nevertheless permitted users to enter passwords that superseded default PVF permission settings, effectively giving users a different profile of permissions. Since our engagement began, Bloomberg has disabled known occurrences of this type and has established a working group to further search its code for any other instances in which passwords can supersede PVF level restrictions. Bloomberg has expressed its intent to disable such instances when discovered.

Recommendations. Opportunities to further improve application security include:

- Monitoring user activity logs with automated triggers and alerts to system and application administrators for the detection of anomalies and timely escalation to management for action;
- Using the newly established working group to search remaining code for any other instances in which passwords might be able to supersede PVF level restrictions; and
- Conducting periodic testing on the implementation of the recently released RBP system.

Additional application security testing

In addition to the application security testing, Promontory performed a series of tests on employee access to Client Data through functions on the terminal. These tests confirmed effective restrictions on access for key data, systems, and functions such as:

- Trading, position, message, and Instant Bloomberg (Bloomberg’s proprietary instant messaging tool) data through the terminal. Bloomberg policy limits access to trading, position, message, and Instant Bloomberg data to personnel who respond to specific client requests, resolve technical issues, price securities, and

perform other roles for which access is required to build, run, and maintain the terminal. These personnel include trade desk application support staff; trading interface support and maintenance specialists; and trading interface developers. From time to time, other specialized application developers; integration and implementation specialists; and financial engineers and quantitative analysts may be granted access to this data on a need-to-know basis. Where appropriate, Bloomberg personnel access is further limited to authorized project and terminal functionality. News reporters and editors are among the many roles not authorized to access this information.

Promontory tested Bloomberg's controls restricting employee access through the terminal to trading, position, message, and Instant Bloomberg data. The testing included identification of terminal functions that potentially provide access to the above data, systematically sampling employees from non-U.S. offices, and a review of such employees' access to the above functions.

Promontory's testing confirmed the access restrictions.

- CRM data on the UUID function and ADSK request information. Promontory completed a test of controls preventing Bloomberg journalists in the News and Multimedia divisions from accessing certain terminal usage data through the terminal, including:
 - CRM data on the UUID function; and
 - ADSK request information, except for news-related queries that are directed to specific journalists.

The testing included identification of terminal functions that potentially provide access to the above data, systematically sampling employees from around the globe, and reviewing such employees' access to the above functions.

Promontory's testing confirmed these access restrictions.

Promontory conducted additional testing of access controls for a number of product groups that permit access to certain types of Client Data. These controls limited access to selected employees within the following workforce roles: Information Security Specialists; Integration and Implementation Specialists; Operations Personnel; R&D Staff; Sales Professionals; Senior Management; and Trade Desk Support Staff.

Promontory's testing validated that only authorized employees were able to access Client Data within the functions associated with these product groups. The products groups tested were:

- Fixed Income Electronic Trading (“FIT”) data. FIT is Bloomberg's fixed income trading platform for U.S. rates and global sovereign debt. FIT links fixed income electronic trading products and provides multi-dealer composite pricing. It allows clients to stage, monitor, trade, and allocate trades.
- Asset and Investment Manager (“AIM”) data. AIM assists buy-side institutions, hedge funds, and proprietary trading desks with decision support and portfolio management; pre-trade, post-execution and end-of-day compliance; order management, electronic trading and execution; and post-trade matching, settlement, reconciliation, portfolio accounting, performance measurement, and data aggregation and reporting.
- Trade Order Management Solutions (“TOMS”) data. For sell-side fixed income firms, TOMS enables users to manage inventory, market making, risk, P&L, and straight-through processing.
- Sell-Side Execution and Order Management Solutions (“SSEOMS”) data. SSEOMS offers sell-side solutions including idea generation, liquidity management, and electronic order flow; market execution, positions, and P&L and risk management; and compliance and middle- and back-office operations.
- Multi-Asset Risk System (“MARS”) data. MARS provides risk management, stress testing, and scenario analysis tools for portfolios containing derivatives and their underlying instruments, including the ability to analyze multiple security types and calculate the profit/loss and various sensitivity indicators for portfolios. MARS features access to Bloomberg's pricing models and market data, including curves, underlying prices, and volatilities.
- Portfolio and Risk Analytics (“PORT”) data. PORT provides tools to understand the structure of portfolios, analyze positions and active bets, and explain the drivers of historical performance and potential sources of future risk. PORT includes intraday performance monitoring, fundamental characteristics, historical performance attribution, ex-ante tracking error, scenario analysis, and portfolio optimization.
- All Pricing Quotes (“ALLQ”) data. ALLQ is a consolidation of all price quotes contributed on a fixed income instrument and, for various asset classes within fixed income, also facilitates electronic trading directly with the contribution source. Dealers and pricing vendors that contribute prices to Bloomberg control access so that only authorized users will see a dealer's name and quote level on ALLQ. Trading is controlled separately via the FIT system.

- Voice Trade Confirmation (“VCON”) data. VCON is a voice trade confirmation system that allows users to match and affirm trades with counterparties. Clients use VCON to send trade recaps to their customers following a trade over the telephone. The customer can then affirm or reject the trade, and it can be allocated like an electronic trade. The trade can also update clients’ position and risk management systems.
- Equity Execution Management System (“EMSX”) data. EMSX provides real-time data, trading, and execution management tools for buy-side and sell-side clients. Clients can access pre-trade analytics to trade single or basket orders, choose the appropriate broker, route to various execution venues, and analyze execution performance.
- Fixed Income Staging Blotter (“TSOX”) data. TSOX provides real-time data, trading and execution management tools for buy-side and sell-side clients for fixed income orders. Clients can manage trade orders and trade ideas, and also share them among fixed income professionals.
- Message Scraping. Message Scraping helps Bloomberg terminal clients bring pricing transparency by allowing them to elect to use their messages as a source for pricing information. Bloomberg Message Scraping uses a proprietary algorithm to extract pricing sent to a client’s inbox so the client can leverage this information to stay abreast of the markets, analyze historic trends, and accurately value positions.
- Tradebook data. Tradebook provides the ability to manage trading strategies in global exchanges for equities, futures, options, and foreign exchange. Tradebook and its affiliates also provide direct market access and trading analytics and algorithms to institutional traders.
- Commission Management Services (“BCMS”) data. BCMS allows clients to trade with multiple brokers and aggregate credits accrued or payments made.
- Trade Ideas Messaging (“TMSG”) data. TMSG allows clients to send investment ideas to other Bloomberg service users, including details such as security recommendations, conviction, target price, and horizon date. TMSG service also allows clients to track, filter, aggregate, and analyze their sent and received ideas.
- Indications of Interest (“IOI”) data. IOI enables potential sellers and buyers of securities to indicate their interest in conducting a transaction to each other. Once a trade is completed, the IOI service enables the broker involved in the

transaction to advertise the trade (and the broker's involvement) to the Bloomberg user community at large.

External to Bloomberg, access to IOI is limited to the parties to whom the communication was directed by the client.

- Data License data. Bloomberg's Data License product leverages the data of the terminal into an enterprise feed that provides descriptive, pricing, corporate action, and analytics data for securities in a client's portfolio or all securities.

Findings. We found application controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

We confirmed that PVF permissioning functions as described. Throughout our work, when PVF levels enabled permission, the employee could, in all cases, access the permitted data; when PVF levels were not enabled, in all cases, the employee could not access the data.

We note that the relative homogeneity of Bloomberg's systems helps to enhance access controls and simplifies the task of administering permissions.

Bloomberg developed a reporting functionality to trace individual grants of PVF permission to an individual's particular job role.

Bloomberg aligned the expiration times for Tradebook functions that allow R&D employees access to restricted data and monitor use of that access for anomalous activity.

Our testing identified instances in which access to restricted data functions, including for trading and position data, was granted on a division-wide basis for certain divisions, including R&D. During the course of our engagement, Bloomberg continued its program for terminating division-level access for restricted data functions. For each of Bloomberg's major product groups tested in conjunction with this review, we validated that Bloomberg migrated all function permissions away from division-level access and instead provided access according to specific sub-roles within divisions.

We also observed that in some cases, functions were categorized in product groups when they were not closely related, making the grouping less intuitive and more difficult to manage.

Recommendations. Opportunities to further improve include:

- Centralizing and documenting function interconnectivity to capture how PVF levels for functions impact permissions afforded to users of other related functions;

- Enhancing data classification procedures and the SDLC to help ensure that there is consistency in and central control over the development of new PVF levels. Bloomberg should also create written documentation governing who can serve as PVF level administrators;
- Extending the practice of displaying a tag demarcating "production" data more widely to differentiate between "live" client and training/demonstration data; this would make it easier to observe and enforce compliance with Bloomberg's data policies;
- Conducting more systematic reviews of user attempts to login into unauthorized functions in order to detect and deter suspicious behavior; and
- Taking inventory on a regular basis of all PVF permission level descriptions to help ensure that PVF administrators have all the facts needed to make a reasoned judgment about the appropriateness of permission settings for all users who are enabled or are seeking to be enabled on the function level.

Database security

Standards. The COBIT Section PO6 provides a framework for standards and procedures intended to safeguard databases against compromises of confidentiality, integrity, and availability. Organizations should establish a security baseline for database systems for future comparison, including planning and risk assessment, host operating system security issues, authentication, access controls, auditing, networking, availability/backup/recovery, and application development. The ability to track and monitor these areas can help an organization identify potential issues, for example, unauthorized access, unpatched systems, excessive privileges, and weak passwords.

Findings. We found database security controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

The IT infrastructure at Bloomberg supports heavy demands for dynamic and real-time information. We observed a centralized Database Administration Group that maintains and supports thousands of databases across the development and production environments. Database administrators use internal systems to access production databases for diagnosing emergency issues and promptly solving them. Database administrators have the ability to self-approve their access to the production servers they support. These activities are restricted to their job functions and are currently logged. The logs are available for ad hoc review, but currently there is no automated system in place that would trigger an alert in the case of a detected anomaly.

Recommendations. Opportunities to further improve database security include:

- Implementing monitoring of activity logs with automated triggers and alerts to system and application administrators for the detection and timely escalation of flagged anomalies to management for action.

Network security

Standards. Network security protects large organizations with complex computer networks and multiple layers of access controls from unauthorized access, malicious activity, and data loss. ISO 27002 Section 10.6 articulates a set of standards governing network management and key security features for organizations to follow. Network security requires effective implementation of various control mechanisms, relative to the complexity of the network, to adequately secure access to systems and data. Network security controls should group systems, applications and users into security domains and establish appropriate access requirements within and between each security domain.

Findings. We found network security controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

The Bloomberg private network is segmented into several security domains running various operating systems (Windows, UNIX, etc.) that govern its systems, data, and users. Bloomberg compartmentalizes and protects its domains, systems, and data from a variety of internal and external threats. We interviewed a number of personnel with operational or management responsibility for aspects of network security. Security software such as anti-virus, intrusion detection, and firewalls are centrally managed and monitored on an intraday basis. Firewall, wireless LAN, and VPN settings are reviewed and approved by management on an as needed basis. Our assessments specifically focused on domains that govern the systems and hardware that house and maintain Client Data.

Recommendations. Opportunities to further improve network security include:

- Implementing a plan, including the development or licensing of technology, for unifying the monitoring of security policy violations and anomalous activity; and
- Establishing 24-hours-a-day, 7-days-per-week security monitoring capabilities to include personnel and infrastructure (e.g., facilities, software, and hardware).

Incident response

Standards. Organizations should maintain policies and procedures to help ensure that a reliable process exists for identifying potential issues and vulnerabilities. ISO 27002 Section

13 outlines the specific components necessary to help ensure that there is effective incident management and remediation. When incidents and vulnerabilities are identified, they need to be triaged, reviewed, escalated, and remediated in a timely manner. Prompt and successful containment and remediation is critical to the protection of the information assets within the organization. The organization should have dedicated security personnel in place to monitor and react to threats on a real-time basis. Incident response procedures should be well documented and appropriate staff trained in their execution.

Findings. We found incident response controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

We reviewed the Incident Response Policy, which includes classification of incident types, handling procedures, mobilization of an incident response team, and escalation to executive management as needed. We met with the information security teams responsible for incident response as well as the team responsible for conducting internal penetration testing. The teams follow similar protocols within the internal ticketing system to identify and escalate incidents and vulnerabilities to the needed R&D resources. We conducted walk-through tests of the penetration testing process, reviewed the management of some past incidents, and observed management of some live incidents that occurred during the course of our review. We were able to observe the interaction between the teams and R&D occurring throughout the process. The requirements for initiating the penetration testing process and standardization of the reviews were not codified within a written procedure. We reviewed evidence of quarterly executive management reporting related to identified vulnerabilities and escalation of high-risk issues but not more frequent monitoring by management for potential trends and patterns, which the COBIT Sections ME1 and ME2 (Monitor and Evaluate IT Performance and Internal Controls) require. All incidents with widespread impact undergo a mandatory post mortem review.

Recommendations. Opportunities to further improve incident response include:

- Drafting written procedures describing the penetration testing process; and
- Aggregating the results of penetration testing and vulnerability assessments into a format that management can regularly and more frequently review in order to identify trends and patterns.

Personnel security

Standards. The Personnel Security section within the FFIEC IT Examination Handbook recommends that organizations mitigate the risks posed by employees, contractors, and third-party vendors by performing appropriate background checks and screenings of new

employees and obtaining agreements covering confidentiality, nondisclosure, and authorized use. Job descriptions and employment agreements increase employee accountability for information security and support policy awareness and compliance. Controls should be in place to help ensure that employees, contractors, and third-party users understand their responsibilities and are well suited to the roles for which they are considered. There should also be controls designed to reduce the risk of theft, fraud, or misuse of facilities or information assets.

Findings. We found personnel security controls to be appropriately designed and implemented.

We reviewed Bloomberg's Global Resource and Information Core Guide, which includes employment related procedures, a code of conduct, and information security guidance. Bloomberg uses the Global Core Guide to instruct its employees on rules of ethics, proper conduct, and responsibilities relating to information security. Under the provisions of the Global Core Guide, employees are held responsible for violations of Bloomberg's policies and code of conduct.

Bloomberg requires employees and contractors to complete comprehensive background checks prior to beginning work, and third-party service providers must do so prior to accessing Bloomberg systems or working at Bloomberg facilities. All personnel coming in contact with proprietary information or confidential data are subject to a confidentiality agreement before being granted access to Bloomberg facilities. Employees leaving Bloomberg are formally reminded of their contractual duty to keep sensitive information confidential and are asked to reaffirm this commitment. Our assessment included a review of documentation, interviews with key staff, and a detailed demonstration of the onboarding and off-boarding processes, including the associated tracking tickets.

Recommendations. None.

Physical security

Standards. Physical security controls should be implemented to prevent unauthorized access to sensitive information, unplanned downtime, and loss of critical data. ISO 27002 Section 9 contains specific guidelines for organizations to follow when designing a physical security program intended to protect critical or sensitive information processing facilities. Physical security controls include maintaining a hardened perimeter, restricting access to facilities, protecting equipment from external and environmental threats, heightened measures for high risk areas like data centers, and maintenance requirements designed to maintain continued availability.

Findings. We found physical security controls to be appropriately designed and substantially implemented, with additional enhancements in progress.

We observed a variety of security controls in place across the multiple Bloomberg sites we visited. Our field work included comprehensive walk-throughs of the two Bloomberg data centers. We noted that while individuals were authenticated at the main entrances, no guard or heightened authentication process is located at the entrance to the data center. These areas were protected by badge readers and closed-circuit television (“CCTV”), which provide limited value in preventing unauthorized individuals from following authorized individuals into these high-risk areas. We reviewed the physical security policy and evaluated resources dedicated to maintaining continuous availability. Security staff monitors the facilities 24 hours a day, 7 days a week, and 365 days a year. This monitoring is supplemented by a suite of security controls, including:

- Physical barriers protecting the perimeters of the facilities;
- Strong methods to authenticate employees, contractors, and visitors prior to granting access to the facilities;
- Regular reviews of employees with access to high-risk areas (e.g., Data Centers); and
- CCTV at all entry and exit points that is both monitored real time and retained for more than 60 days.

In addition to the physical mechanisms noted above, Bloomberg maintains appropriate environmental controls at its data centers to reduce the likelihood of outage or data loss. The environmental controls include:

- Raised flooring;
- Redundant cooling systems;
- Fire suppression;
- Fluid and moisture detection;
- Redundant Uninterruptable Power Supply Units (UPS);
- Multiple power, telecommunications, and network feeds;
- Redundant generators; and
- Service-level agreements with multiple fuel vendors (both local and national).

Recommendations. Opportunities to further improve physical security include:

- Implementing additional mechanisms to prevent unauthorized entry into data centers.

Vendor management

Standards. Organizations should have processes in place regarding the selection, contracting, and oversight of third-party vendors to identify and mitigate any risks a vendor may present to the organization while providing products or services. ISO 27002 Section 10.2 provides guidelines designed to help ensure that the level of information security maintained by third parties is appropriate for the services provided, and is monitored and reviewed with regular frequency. This includes assessing the risk associated with vendors who come into contact with sensitive information or perform services critical to the organization. Vendor management controls should include a mechanism to assess vendors using a risk-based approach, and sufficient risk assessments based on the services provided and data access required. Identified risks should be communicated to the business unit and management in a timely manner, followed up on, and remediated or accepted.

Findings. We found that Bloomberg has vendor management controls that are appropriately designed and that recent enhancements to those controls are being implemented.

Vendor management at Bloomberg, like vendor management at many financial institutions with which we are familiar, is expanding from a process that was focused on due diligence at procurement to a more formal, risk-based program for the selection, contracting, and ongoing oversight of vendors.

Bloomberg does have a vendor security risk assessment process in place that is currently performed by the Security division. Documentation and practices exist around conducting vendor due diligence. The Risk division relies on business units to proactively notify them about new vendor relationships and request security risk assessments. During our walk-through, we observed that the assessments are conducted across three different systems, which appears to add unnecessary complexity to the process. There is evidence of vendors being tiered based on the results of a security survey, with tailored assessments conducted on high risk vendors. Results of the assessments are communicated back to the applicable business unit and any needed corrective action is taken. Vendors are required to sign non-disclosure agreements designed to enforce baseline security standards, and certain vendors are asked to execute security addenda.

Bloomberg is implementing an enterprise-wide process supported by central coordination, for the selection, contracting, and oversight of vendors.

Recommendations. Opportunities to further improve vendor management include:

- Implementing an enterprise-wide vendor management program to provide a risk-based framework for the selection, contracting, and oversight of vendors through a unified security risk assessment process;
- Centralizing the administration and oversight of the program to help ensure adoption and consistency; and
- Consolidating the number of systems used for security risk assessments of third-party vendors.

Privacy

Standards. An organization-wide privacy program should be effective to enable compliance with applicable privacy laws and regulations and help align the organization's approach to privacy with generally accepted frameworks such as the FIPPs and Privacy-by-Design ("PbD"). Characteristics of an effective program include: periodic identification and assessment of privacy-related compliance obligations and risks; regular reviews and updates of organizational privacy policies and procedures; the inclusion of relevant privacy concepts in workforce training; implementation of reasonable technological and procedural controls to help protect and manage personally identifiable information in accordance with the organization's policies and obligations; a protocol for handling potential data security incidents; the allocation of accountability to an appropriate member of senior management; and identification and support of program advocates, who, in their parts of the organization, are responsible for implementing relevant portions of the privacy program.

Findings. Bloomberg's Personal Client Data privacy program is appropriately designed and implemented, with additional enhancements in progress. Bloomberg has an existing core privacy compliance team, and draws upon legal advisors in multiple jurisdictions to assist in providing regulatory notifications and developing global practices that take into account country-specific data protection requirements and regulators' guidance. There is an incident response process that encompasses personal client data. Data privacy and security training is in progress for the entire workforce.

Bloomberg's Personal Client Data Privacy Policy helps create an organization-wide framework to unify varying local and business unit approaches to data privacy, which should enhance Bloomberg's ability to identify, assess, and address privacy-related risk in a rapidly evolving technology, business and regulatory environment.

A Privacy Notice for the terminal describes the types of personal information collected and the uses of the information collected; it also discloses that the information may be accessed

outside the country of origin by Bloomberg employees worldwide. There are other privacy notices in place across different product areas.

The presence of personal Client Data within Bloomberg was a factor considered during the development of Bloomberg's Client Data Classification Policy and its supporting procedures. As such, our findings and recommendations regarding the data classification process and access controls are also relevant when considering Bloomberg's management of privacy.

With respect to certain categories of personal Client Data, Bloomberg has certified its compliance with Safe Harbor under the U.S. Department of Commerce regarding data transferred from the European Union and European Economic Area to the United States and from Switzerland to the United States.

Bloomberg is planning to add specialized resources to the core privacy team and has included this in the current, approved, resourcing plans.

Recommendations. Opportunities to further improve the privacy program include:

- Documenting a unified set of procedures that support the existing Personal Client Data Privacy Policy and draw upon existing compliance practices and documentation where possible;
- Expand and support the organization-wide approach to supporting the Personal Client Data Privacy Policy; and
- Implementing the current plan to add privacy staff resources.

Training

Standards. A firm-wide training program should give consideration to:

- Initial training for personnel addressing the importance of handling Client Data appropriately;
- Ongoing awareness activities targeting personnel as appropriate;
- Training modules tailored for specific workforce roles;
- Refresher training for all personnel on a periodic basis; and
- Robust tracking of personnel training via a learning management system to help ensure that personnel complete required training modules.

Consideration should be given to the need to tailor training to workforce roles and the risk associated with those roles. Training modules and their mode of dissemination should be designed to communicate materials effectively to personnel.

The delivery and scope of the training should be monitored for completeness. Metrics, such as post-training testing, surveys, and the frequency of subsequent incidents should be used to assess the effectiveness of training.

Findings. Bloomberg University (“BU”) is the central portal for all online training for all personnel. New hires undergo a two-day induction and are required to complete a number of training modules involving the code of conduct and compliance with Bloomberg’s policies. Bloomberg has recently implemented a plan for a newly developed, mandatory, firm-wide training program that emphasizes information security and compliance with Bloomberg policies.

During July and August 2013, Bloomberg began developing an Information Security Training Program for all Bloomberg personnel that incorporates the requirements of Bloomberg’s Client Data Principles and Policies. The Information Security Training Program has been initiated, with the first classroom-led training courses being held in New York.

The first phase of the Information Security Training Program has been launched with four mandatory modules targeted at selected groups of Bloomberg personnel:

- Security and privacy for managers (including a video message from the CEO and the Chairman);
- Security and privacy for human resources staff;
- Specialist training for BAR personnel (in-business staff who administer access permissions); and
- Specialist training for managers with access control authority.

All courses in the Information Security Training Program are administered via BU. BU tracks requirements, due dates, and attendance, and sends notifications to personnel and their managers.

We have reviewed the overall training program plan and understand that feedback from the first phase of the training program will be collected in late September. The content will be adapted for a broader audience of all Bloomberg personnel and will incorporate feedback from the initial phase. This content will form the basis of an online mandatory information security training course for all personnel which will be launched in November, for completion

by all personnel by the end of 2013. Firm-wide training on privacy and Client Data issues is supplemented with tailored training modules for specific workforce roles.

Bloomberg is also in the process of updating its new-hire training curriculum to reflect new policies, procedures, and responsibilities for all personnel. New content will be added to the live orientation program presented to employees on their first day at Bloomberg, and an online course for new hires will be launched in 2013.

Bloomberg has added staff to their training division and has engaged an external training development vendor to assist in the development of online training modules.

Following the rollout of the online training, Bloomberg intends to institute a program of refresher trainings with annual re-certifications via its Learning Management System.

Recommendations. Opportunities to further improve Bloomberg's training of personnel include:

- Continuing to follow the current Security and Privacy Training roadmap;
- Including quiz sections in the planned training for all Bloomberg personnel to test staff comprehension of the key messages of the training; and
- Developing the current planned program metrics into a series of "business as usual" metrics that can be used to inform management regarding the ongoing awareness of Bloomberg's Client Data Policies and Procedures and to assess opportunities for improvement in the current Training Program.

Accountability

Standards. Key accountability standards of particular relevance to Bloomberg are described below.

Personnel should be aware of the standards of behavior to which Bloomberg expects them to adhere, including the detailed, unambiguous expectations and requirements articulated in policy documents and communicated through training.

All personnel should be aware of their personal accountability and responsibility for handling Client Data appropriately in their work.

Personnel should be encouraged to seek clarification and support if they are unsure what they should do in any situation involving the handling of Client Data. In addition, personnel should be encouraged to escalate issues that they believe may result in risks to Client Data.

Compensation policies and practices should include consideration of employees' contributions to meeting risk and compliance goals.

There should be clear consequences for any personnel who breach the principles, policies, and procedures in place. Depending on the severity of the breach, the consequences may involve disciplinary action, including counseling, probation, suspension, or dismissal.

Findings. Bloomberg has clear Client Data policies and procedures in place. These policies clearly establish responsibilities of personnel and provide for disciplinary action up to and including dismissal for violations.

Bloomberg had a whistleblowing hotline in place prior to Spring 2013, but it was not well publicized. Bloomberg is increasing the number of staff supporting the hotline, the hotline is included in the current personnel training material, and the hotline will be publicized as part of the all-personnel training to be rolled out later this year.

As noted above, Bloomberg policies permitted journalists to view UUID and ADSK screens prior to Spring 2013. As such, reporters and editors have not been formally disciplined for this practice. However, we understand that the Clark Hoyt's report will recommend the creation of an Standards and Practices Task Force that will, among other things, consider the need for additional training for reporters and editors.

Bloomberg is enhancing its performance evaluation process to more fully consider employees' contributions to risk and compliance goals.

The newly constituted Audit, Risk & Compliance Committee will oversee Bloomberg's implementation of accountability mechanisms.

Recommendations. Opportunities to further improve Bloomberg's enforcement of accountability and consequences include:

- Enhancing the performance evaluation process to more fully consider employees' contributions to risk and compliance goals; and
- Better publicizing the whistleblowing hotline.

C. Review of Enhancement Plans

In this section, we report our assessment of Bloomberg's plan to enhance its framework and controls going forward, including its prospective testing methodology.

Description of Enhancement Plans

Bloomberg has plans to enhance its Client Data controls going forward, including:

- Establishing a Chief Risk and Compliance Officer;
- Completing the formalization of procedures implementing the Client Data Policies; and
- The CDCO Roadmap.

The first two of these plans have been discussed above.

The CDCO Roadmap outlines Bloomberg's plans to continue enhancing its Client Data controls. The Roadmap is a detailed list of activities that are either specific responses to our recommendations or additional self-identified opportunities for improvement. They can be categorized as either:

- Short-term activities to be completed within the next sixty days. These activities all have named resources allocated to them and specific deadlines for completion; or
- Longer-term activities, to be completed after the next sixty days. The planning for these activities is still ongoing and the planning is expected to be complete within ninety days. As stated elsewhere in the Report, Bloomberg has accepted all of our recommendations.

We reviewed the Roadmap and determined that all of our recommendations contained in this Report have been addressed. The activities appear reasonable and align with our understanding of Bloomberg's overall enhancement plans. The prioritization and allocation of activities between short and longer terms activities also appears reasonable.

In August 2013, Bloomberg's Management Committee received and approved resourcing requests for staffing to support Client Data risk management activities in 2013-2014, with additional resources allocated to the CDCO, Legal, Vendor Management, and the Security function.

Description of Bloomberg's Prospective Testing Methodology

Bloomberg proposes to adopt a risk-based monitoring and testing methodology. The proposed methodology incorporates control owners monitoring the effectiveness of their controls, periodic testing of controls, reviews by Internal Audit, and third-party reviews:

- **Monitoring.** Control owners will perform ongoing monitoring of the effectiveness of the Client Data compliance controls they own (e.g., the owner of the Walled Garden will monitor the Garden to help ensure that unauthorized users do not gain access and that authorized users confine their access to approved purposes). Each information security asset owner will be responsible for describing the monitoring that will be conducted in connection with the owner's inventory of information security assets.
 - Performed by: The owner of the control (often line-of-business management and R&D management, but sometimes compliance or security functions where they administer a control directly).
 - Resources: Monitoring will primarily be performed by internal Bloomberg resources.
- **Testing.** Risk and Compliance functions will perform periodic testing of the effectiveness of Client Data compliance controls. When Risk and Compliance is the control owner the testing will be done by an independent resource from outside of the Risk and Compliance division. The frequency of the testing will be determined based on the risk assessment conducted pursuant to the Information Security Policy. In most cases, this testing will be done with less frequency than monitoring. Risk and Compliance functions may use internal or external resources to conduct the testing as appropriate. For the initial year, Risk and Compliance will rely on testing performed by Promontory as part of this review and augment that testing to include controls added after the date of this Report or controls that were not part of the key controls tested by Promontory.

A tentative schedule of testing by the Risk and Compliance functions from September 2013 to September 2014 is being drafted, and Bloomberg intends to finalize the schedule upon completion of the information security risk assessment described above.

- Performed by: Risk and Compliance functions.
 - Resources: Testing will primarily be performed by a mix of internal Bloomberg resources and external experts with special skills, such as penetration testing. Especially in the first year, Risk and Compliance may rely on testing performed by third parties.
- **Internal Audits.** The Internal Audit function will audit compliance with Client Data policies and procedures. The Internal Audit function will conduct its own

assessment of the information security risks facing Bloomberg. It will then use the results of that assessment to audit the risk assessment conducted by the Risk and Compliance function. Further, it will use the assessment to determine the frequency of audits of policies and procedures by business units. However, Internal Audit will help ensure that compliance with each policy and procedure is audited at least once every three years with respect to most business units and Bloomberg locations. Internal Audit may use internal or external resources to conduct their audits as appropriate.

In addition, following the issuance of the Report, the Audit, Risk & Compliance Committee will ask Internal Audit to undertake a follow-up review. This review will assess Bloomberg's progress in implementing the enhancement plans identified above and in addressing the recommendations of this Report. The review will also develop recommendations for the scope and nature of an ongoing periodic third-party Client Data review program (see below).

- Performed by: Internal Audit.
- Resources: Audits will be performed by Internal Audit using primarily internal resources with outsourcing or co-sourcing to external firms as appropriate or necessary depending on Internal Audit's resource availability and expertise.
- **Third-Party Reviews.** Bloomberg is committed to regular third-party reviews of its Client Data and information security programs. The results of these reviews will be made available to clients.

Upon completion of the follow-up review of this Report by Internal Audit, the Audit, Risk & Compliance Committee will consider Internal Audit's recommendations for the third-party Client Data review program and will initiate the program.

Although the scope and approach of these reviews will be at the discretion of the Audit, Risk & Compliance Committee, it is anticipated that they will include:

- Ongoing testing of Bloomberg's information security controls, which will further develop the testing framework used in this Report. It is anticipated that this testing will include:
 - Reviews of penetration testing, including network testing, social engineering, and physical security;
 - Static and dynamic code review; and

- IT general controls, including application security, change management, and incident response.
- Ongoing testing of employee access to specific functions on the terminal.

Findings. Hogan Lovells and Promontory assisted Bloomberg in the formulation of these enhancement plans and prospective testing methodologies and find them to be reasonable, realistic, and a sound basis for managing the risks to Client Data in their respective areas.

Recommendations. Opportunities to further enhance Bloomberg's plans for improvement include:

- Adopting a consolidated process for tracking implementation of Bloomberg's enhancement plans; and
- Adopting a consolidated process and system for tracking the results of the monitoring, testing, internal audits, and third-party reviews, including issues identified.

8. Appendices

Appendix A

Hogan Lovells and Promontory's Terms of Reference

Bloomberg L.P. (the "Company") has engaged Hogan Lovells US LLP ("Hogan Lovells") and Promontory Financial Group ("Promontory") to undertake an external review of current practices and policies for client data and end user information ("client data practices and policies"), including past access issues recently raised by the Company's clients.

Hogan Lovells and Promontory will make recommendations and advise Company management on the implementation of enhancements to client data practices and policies, including the independent and ongoing audit or verification of the Company's systems and procedures. Hogan Lovells and Promontory will further:

1. Review the prior practices of the Company with respect to client data policies and procedures;
2. Review the Company's responses to any concerns with prior client data policy or practices;
3. Review the current state of client data policies and procedures at the Company;
4. Review any proposed changes to the Company's policies and procedures relating to client data privacy; and
5. Prepare a report on the above, including findings, recommendations, and advice to support the Company's goal to become an industry leader in this field.

To carry out these objectives, Hogan Lovells and Promontory are authorized to:

1. Review any Company documents or records;
2. Interview Company employees, clients and other constituents;
3. Utilize any Company employee as required by their review; and
4. Consult with, and receive direction from, Samuel J. Palmisano, retired Chairman and CEO of IBM and independent advisor on these matters to the Board of Directors of the Company.

It is the intention of the Company that the Company's in-house counsel and other outside counsel work closely with Hogan Lovells and Promontory and provide all assistance they

require. All Company employees are directed to cooperate fully with Hogan Lovells and Promontory.

As one of the goals of this review is to provide transparency into the Company's client data practices and policies, it is the intention of the Company that upon the completion of Hogan Lovells and Promontory's review the Company will share with its clients and the public the key findings, conclusions, and recommendations of this review.

Effective May 16, 2013

Appendix B

Statement of Samuel J. Palmisano, Independent Advisor to the Board of Directors of Bloomberg L.P., on the Hogan Lovells/Promontory Report

August 20, 2013

In May 2013 I was asked by the Board of Directors of Bloomberg L.P. to provide independent advice on the Company's client data policies and practices.

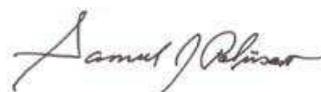
In order to assess the situation, I met extensively with members of the Company's Board, the management team, and representatives of Hogan Lovells US LLP and Promontory Financial Group, the two outside firms engaged to conduct the review. I also had conversations with some of the Company's clients. The Company answered all my questions and always provided access to the people and information I requested.

I made clear that the review needed to address three questions. First, what access did journalists previously have to client data. Second, what had Bloomberg done to correct the situation and prevent inappropriate access to client data. And third, what had Bloomberg done to address client data security and privacy comprehensively going forward.

The Report issued today is thorough, objective, and comprehensive. It clearly answers each of my questions. It gives Bloomberg's clients a precise sense of what happened and why, what Bloomberg has done to prevent future occurrences, and how the Company plans to continue to improve.

Bloomberg's leadership recognized the need for a more comprehensive set of policies and procedures. They acted quickly to enhance their existing structures and put more resources behind this critical priority. Based on my own observations, I support the Report's conclusion that Bloomberg currently has appropriate policies and controls in place.

The Company's leadership also recognizes that they can do even better and is on the path to create a new industry standard. Enhanced governance, independent audits, and improved training will help ensure that the Company avoids making this kind of mistake again. The Report lays out a clear set of recommendations in these and other areas along with the Company's specific responses. This is the kind of clarity, accountability, and commitment Bloomberg's clients deserve.



Samuel J. Palmisano
Norwalk, Connecticut

Appendix C

List of Recommendations

Recommendations	Management Response	Status
Retrospective Review		
<i>Journalist Access</i>		
The News division should provide appropriate training and create formal plans for reexamining policies and key issues related to client privacy expectations.	Accepted	In Progress
Bloomberg should continue to restrict journalist access to ADSK tickets. Journalists should, however, be permitted to view and respond to ADSK inquiries related to articles they have written.	Accepted	In Progress
Bloomberg should enhance its training program to help ensure that personnel understand the restrictions on access to and use of password-protected information regarding mortgage-backed instruments.	Accepted	In Progress
To the extent that Bloomberg decides to allow journalists to access anonymous Bloomberg chat rooms in the future, Bloomberg should explicitly notify terminal users that Bloomberg journalists may be viewing the chats and provide clear, written instructions to journalists regarding what constitutes acceptable conduct.	Accepted	In Progress
Review of Client Responses and Public Statements		
<i>Steps to Clarify Statements in Client Responses</i>		
Bloomberg should adopt a more-regular practice of reminding its employees of their Client Data confidentiality obligations.	Accepted	In Progress
Review of Current Client Data Policies and Practices		
<i>Tone at the Top</i>		
Bloomberg should continue to cascade the tone at the top established by senior executives and support Bloomberg's efforts to enhance its culture around risk and compliance. This is particularly important in the news businesses.	Accepted	In Progress
Bloomberg should maintain its respectful attitude toward risk and compliance professionals and the need for a strong internal audit function.	Accepted	In Progress

Recommendations	Management Response	Status
<i>Governance</i>		
Bloomberg should maintain a majority of members of the Audit, Risk & Compliance Committee who are independent.	Accepted	Complete
Bloomberg should periodically assess the effectiveness and mandate of the Audit, Risk & Compliance Committee, including determining whether the members of the Audit, Risk & Compliance Committee have the time, requisite experience, and resources necessary to make the Committee effective.	Accepted	In Progress
Bloomberg should fill the newly created position of Chief Risk and Compliance Officer with a qualified person and provide the position with an adequate staff and budget, sufficient stature and authority within the organization, and access to data and other resources needed to assess the state of Client Data controls.	Accepted	In Progress
Bloomberg should develop a migration plan to transform CDCO from a change program into a "business as usual" division.	Accepted	In Progress
Bloomberg should complete the implementation of the governance-related components of the Information Security Policy, particularly the information security risk assessment. This risk assessment should build on the testing performed in the course of our review. Bloomberg should use the results of the risk assessment to further enhance its information security risk-management program.	Accepted	In Progress
Bloomberg should establish and staff an independent, internal audit function with appropriate resources in terms of both quantity and qualifications.	Accepted	In Progress
Bloomberg should charge the Audit, Risk & Compliance Committee with the task, going forward, of validating that the approved recommendations of this Report have been implemented fully.	Accepted	Complete
Bloomberg should implement better mechanisms for tracking and following up on recommendations from external and internal sources, including implementation of the recommendations arising from this Report.	Accepted	In Progress
<i>Policy and Procedure Design and Content</i>		
Bloomberg should finalize the procedures required to support its Client Data policies.	Accepted	In Progress
Bloomberg should complete the plan to provide personnel with a tailored set of policies and procedures relevant to workforce roles via the terminal.	Accepted	Complete

Recommendations	Management Response	Status
Bloomberg should stagger the review of the recently formalized policies and procedures to spread the review work across the year (this will require reviewing some of the recently formalized policies before their one-year anniversary date).	Accepted	Complete
Implementation of Key Controls - Data Classification, Encryption, and Retention		
Bloomberg should complete the data retention procedures that support the Records Retention Policy.	Accepted	In Progress
Bloomberg should implement technical controls and allocate additional resourcing for CDCO and Legal to enforce applicable data end-of-life procedures in accordance with the Record Retention Policy (and the supporting data retention procedures when they are completed).	Accepted	In Progress
Bloomberg should expand the Client Data Classification Policy to include additional data types such as employee and proprietary data.	Accepted	In Progress
Implementation of Key Controls - Change Management/SDLC		
Bloomberg should develop a plan to enhance the segregation controls between development, test, and production environments.	Accepted	In Progress
Bloomberg should enhance its development and testing environments to more closely mirror its production environment.	Accepted	In Progress
Bloomberg should consolidate the systems for tracking changes to software code.	Accepted	In Progress
Bloomberg should document the change management and systems development life cycle processes to provide clarity and consistent application of authorized approaches and to determine whether appropriate groups are engaged throughout the process.	Accepted	In Progress
Bloomberg should regularly review and audit production access ticketing systems for policy compliance.	Accepted	In Progress
Bloomberg should monitor developer activity logs for irregular or inappropriate activity.	Accepted	In Progress
Implementation of Key Controls - Application Security		
Bloomberg should monitor user activity logs, employing automated triggers and alerts to system and application administrators for the detection and timely escalation of flagged anomalies to management for action.	Accepted	In Progress

Recommendations	Management Response	Status
Bloomberg should use the newly established working group to search remaining code for any other instances in which passwords might be able to supersede PVF level restrictions	Accepted	In Progress
Bloomberg should conduct periodic testing on the implementation of the recently released RBP system.	Accepted	In Progress
Bloomberg should centralize and document function interconnectivity to capture how PVF levels for functions impact permissions afforded to users of other related functions.	Accepted	Complete
Bloomberg should enhance data classification procedures and the systems development lifecycle to help ensure that there is consistency in and central control over the development of new PVF levels. Bloomberg should also create written documentation governing who can serve as PVF level administrators.	Accepted	In Progress
Bloomberg should extend the practice of displaying a tag demarcating "production" data more widely to differentiate between "live" client data and training/demonstration data.	Accepted	In Progress
Bloomberg should conduct more systematic reviews of user attempts to login into unauthorized functions in order to detect and deter suspicious behavior.	Accepted	In Progress
Bloomberg should take inventory on a regular basis of all PVF level descriptions to help ensure that PVF administrators have all the facts needed to make a reasoned judgment about the appropriateness of permission settings for all users that are enabled or are seeking to be enabled on the function level.	Accepted	Complete
Implementation of Key Controls - Database Security		
Bloomberg should implement monitoring of activity logs with automated triggers and alerts to system and application administrators for the detection and timely escalation of flagged anomalies to management for action.	Accepted	In Progress
Implementation of Key Controls - Network Security		
Bloomberg should implement a plan, including the development or licensing of technology, for unifying monitoring of security policy violations and anomalous activity.	Accepted	In Progress
Bloomberg should establish 24-hours-a-day, 7-days-per-week security monitoring capabilities to include personnel and infrastructure (e.g., facilities, software, and hardware).	Accepted	In Progress

Recommendations	Management Response	Status
Implementation of Key Controls - Incident Response		
Bloomberg should draft written procedures describing the penetration testing process.	Accepted	Complete
Bloomberg should aggregate the results of penetration testing and vulnerability assessments into a format that management can regularly and more frequently review in order to identify trends and patterns.	Accepted	In Progress
Implementation of Key Controls - Physical Security		
Bloomberg should implement additional mechanisms to prevent unauthorized entry into data centers.	Accepted	Complete
Implementation of Key Controls - Vendor Management		
Bloomberg should implement an enterprise-wide vendor management program to provide a risk-based framework for the selection, contracting, and oversight of vendors through a unified security risk assessment process.	Accepted	In Progress
Bloomberg should centralize the administration and oversight of the enterprise-wide vendor management program to help ensure adoption and consistency.	Accepted	In Progress
Bloomberg should consolidate the number of systems used for security risk assessments of third-party vendors.	Accepted	In Progress
Implementation of Key Controls - Privacy		
Bloomberg should document a unified set of procedures that support the existing Personal Client Data Privacy Policy and draw upon existing compliance practices and documentation where possible.	Accepted	In Progress
Bloomberg should expand and support the organization-wide approach to supporting the Personal Client Data Privacy Policy.	Accepted	In Progress
Bloomberg should implement the current plan to add privacy staff resources.	Accepted	In Progress
Training		
Bloomberg should continue to follow the current Security and Privacy Training roadmap.	Accepted	In Progress
Bloomberg should include quiz sections in the planned training for all Bloomberg personnel to test staff comprehension of the key messages of the training.	Accepted	Complete

Recommendations	Management Response	Status
Bloomberg should develop the current planned training program metrics into a series of “business as usual” metrics that can be used to inform management regarding the ongoing awareness of Bloomberg’s Client Data Policies and Procedures and to assess opportunities for improvement in the current Training Program.	Accepted	In Progress
<i>Accountability</i>		
Bloomberg should enhance the performance evaluation process to more fully consider employees’ contributions to risk and compliance goals.	Accepted	In Progress
Bloomberg should better publicize the whistleblowing hotline.	Accepted	In Progress
<i>Review of Enhancements</i>		
Bloomberg should adopt a consolidated process for tracking implementation of the enhancement plans.	Accepted	Complete
Bloomberg should adopt a consolidated process and system for tracking the results of the monitoring, testing, internal audits, and third-party reviews, including issues identified.	Accepted	In Progress

Appendix D

Mr. Doctoroff's Blog Posts Addressing Client Data Issues



LISTENING TO OUR CLIENTS



There's nothing more important to us at Bloomberg than communicating openly and honestly about our company. As such, I'm starting this blog to speak personally and directly to our clients, employees and partners.

Last Friday, I sent a [note](#) acknowledging that we made a mistake in allowing journalists access to limited high-level client relationship data. I also detailed the steps we've taken going forward, including limiting reporter access to only the information available publicly to all terminal users; and creating a new position of Client Data Compliance Officer, reporting directly to me, who is responsible for centralizing our data security efforts.

Since the news came out, my executive team and I have personally reached out to more than 300 clients. We started each conversation with an apology for our mistake. We've listened carefully and also explained the very specific and limited nature of the data our reporters were able to access. We've reiterated what data was available, how it was used, and just as importantly, what was not accessible, including messaging, trading, portfolio, monitor, blotter and other related systems. We're grateful for the understanding our clients have shown.

Let me reemphasize that our company's core value of openness and client trust are our highest priorities and the cornerstone of our business. We will do everything possible to ensure the integrity and confidentiality of our clients' data in all situations and at all times. We are available to all of our 315,000 subscribers to answer any questions or concerns. Please don't hesitate to email me directly at ddoctoroff1@bloomberg.net.

>> Posted by Dan Doctoroff on May 13, 2013

RESPONDING TO A COMMON QUESTION



When I launched my blog, I sent a note to every one of our 315,000 terminal subscribers informing them of it and inviting them to email me directly with questions, comments or concerns. I'm trying to respond to each of them directly or through a personal call or visit from a Bloomberg representative.

By far the most common question I've received is exactly what was the nature of the data our reporters were able to view. Here's a description.

Prior to last month, reporters could access customer relationship management (CRM) information that contains certain data not available on the Bloomberg to all terminal users, such as:

- Login Creation Date – this provides information on when a client initiated usage of a Bloomberg terminal.
- Login History – this provides information on when a user logged into the terminal.
- High Level Usage Data – this provides information on functions used – aggregated over time – with no ability to look into specific security information.
- Help Desk Inquiries – this contains information about customer inquiries and requests. This was typically used to answer client inquiries to reporters about news stories.

It's just as important to know what reporters did not have access to: trading, portfolio, monitor, blotter or other related systems, or client messages. Moreover, reporters could not see news stories read by individual users or any of the securities that clients might be looking at.

And to be clear, reporters now only have access to the same client information as any Bloomberg client.

More to come as I continue to work my way through your questions.

>> Posted by Dan Doctoroff on May 15, 2013

AN INDEPENDENT REVIEW



When it comes to privacy and security, our goal is to set the highest standard.

I'm pleased to announce that Bloomberg has appointed Samuel Palmisano, former Chairman and CEO of IBM, to serve as an independent adviser regarding the company's privacy and data standards and make recommendations on possible enhancements.

We have also appointed Clark Hoyt to review Bloomberg News' relationship with the Company's commercial operations.

Please read our [press release](#).

>> Posted by Dan Doctoroff on May 17, 2013

FAQ ON SAM PALMISANO AND CLARK HOYT REVIEWS



In an earlier [post](#), I announced the appointment of Sam Palmisano to serve as an independent adviser regarding the company's privacy and data standards and to make recommendations on possible enhancements. I also announced the appointment of Clark Hoyt to review Bloomberg News' relationship with the company's commercial operations. Here are answers to some common questions that provide additional information about the scope and details of their reviews:

Question: Will the results of Mr. Palmisano's independent review be shared with clients?

Answer: Yes. The goal of the review is to provide transparency into our client data practices and policies and to implement Mr. Palmisano's recommendations. Upon the completion of Mr. Palmisano's review, the Company will share with our clients his findings, conclusions, and recommendations.

Question: When will Mr. Palmisano complete his review?

Answer: Because Mr. Palmisano will have substantial authority and discretion to shape his review as he sees fit, we cannot state the exact timeline for completion of the review and publication of results. However, the Board has made clear to Mr. Palmisano its desire to move as expeditiously as is appropriate and possible.

Question: Will the Company audit and verify its client data and privacy practices and procedures?

Answer: Yes. The Company is committed to rigorous and regular audit and verification procedures. As part of his review, Mr. Palmisano will review whether the Company has appropriate audit and verification procedures both at the time of his review and on an ongoing basis.

Question: Will Mr. Palmisano's review include an examination of reporter access to client data?

Answer: Yes. Mr. Palmisano will report on how client data was accessed by reporters and ways in which such data was used.

Question: How will Mr. Hoyt's review relate to Mr. Palmisano's?

Answer: Mr. Hoyt will examine the relationship between the Company's news and commercial operations, and make recommendations about appropriate policies and procedures including any structural changes. Messrs. Palmisano and Hoyt will liaise on an ongoing basis and their reviews will occur contemporaneously.

>> Posted by Dan Doctoroff on June 3, 2013

THE REVIEW PROCESS AT THE HALF-WAY MARK



In the month and a half since we announced our plans for an independent companywide review of client privacy and data standards, we've made good progress. I thought I'd provide an update on that progress and the timeline for completing the work and announcing the results, which we plan to do by September 1st.

As I've written about previously, Bloomberg has launched a comprehensive review of our client data policies and practices. The review is being undertaken by teams from Promontory Financial Group and Hogan Lovells with direction from Samuel Palmisano. Promontory and Hogan Lovells both have full-time teams, onsite at Bloomberg and offsite, reviewing past practices, current policies and procedures, and developing recommendations for future changes.

The teams onsite have tested terminal functions that potentially provide access to the most sensitive client data, and they have tested the controls restricting Bloomberg journalist access to certain client usage data, including information on the UUID function and help desk requests.

While the testing of these data access controls is continuing, the initial findings have confirmed that our controls are functioning properly to restrict access to the highest-sensitivity data such as trading, position and message data. These tests have also confirmed that journalists no longer have access to customer relationship management data on the UUID function and help desk requests, except where directed to a journalist to answer a news-related question.

When all testing and other work are completed, the final report resulting from the review will focus on four main areas:

1. Bloomberg's prior client data practices.

Hogan Lovells and Promontory are reviewing past journalist access to certain types of client data, such as login creation date, login history, basic usage data and help desk inquiries.

2. Bloomberg's response to customer concerns.

Hogan Lovells and Promontory are reviewing our company's response to client inquiries, and will evaluate whether we have communicated important information in an effective, forthcoming manner.

3. Companywide policies as of report release.

The Hogan/Promontory review will evaluate whether our current practices, policies and standards reflect our commitment to privacy and confidentiality. In addition, the report will assess whether Bloomberg's organizational structure, management and staffing support these principles, especially with regard to data classification, access control, IT security, training, incident response, physical security and privacy.

4. Plans for enhancements going forward.

Finally, in addition to reviewing current operations, Hogan Lovells and Promontory will make recommendations for how we can make enhancements to set the highest standard in the future. The report will assess our plan for independent verification of our policies and procedures, which we expect will include an independent and ongoing audit for systems and procedures.

News and Commercial Relationship Review

In addition to the review of our data policies and procedures, a team led by Clark Hoyt has been reviewing Bloomberg News' relationship with our company's commercial operations. This has included an examination of practices and policies across news content teams and a review of current policies, procedures and training. So far Clark and his team have conducted more than 100 interviews with Bloomberg News journalists, other Bloomberg employees, clients and other stakeholders.

Sharing the Reports

Based on the progress of our reviews thus far, we intend to share the key findings, conclusions, and recommendations of Promontory and Hogan Lovells' review by September 1st. In the meantime, I'll continue to provide periodic updates throughout the summer.

>> Posted by Dan Doctoroff on July 8, 2013

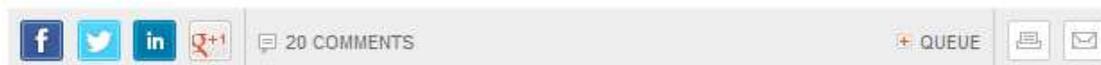
Appendix E

Mr. Winkler's Opinion Piece



Holding Ourselves Accountable

By Matthew Winkler | May 13, 2013 12:11 AM ET



As I wrote in "The Bloomberg Way," our guide for reporters and editors, "The appearance of impropriety can be as damaging to a reputation as doing something improper. Because we hold others accountable for disclosure, we expect the same of ourselves. While disclosing errors of judgment may be embarrassing, the sooner the lapses are reported, the sooner there is nothing more to say."

We are defined by our words -- and they applied to us when a Bloomberg LP customer expressed concern that [Bloomberg News](#) reporters had access to limited client information. Our client is right. Our reporters should not have access to any data considered proprietary. I am sorry they did. The error is inexcusable. Last month, we immediately changed our policy so that reporters now have no greater access to information than our customers have. Removing this access will have no effect on Bloomberg news-gathering.

Now let's also be clear what our reporters had access to. First, they could see a user's login history and when a login was created. Second, they could see high-level types of user functions on an aggregated basis, with no ability to look into specific security information. This is akin to being able to see how many times someone used Microsoft Word vs. Excel. And, finally, they could see information about help desk inquiries.

Why did reporters have access to this in the first place? The recent complaints go to practices that are almost as old as Bloomberg News. Since the 1990s, some reporters have used the terminal to obtain, as the *Washington Post* reported, "mundane" facts such as log-on information. There was good reason for this, as our reporters used to go to clients in the early days of the company and ask them what topics they wanted to see covered. Understanding how clients used the terminal was more important then. We still do that today, which is why we have feedback tabs on our news-related terminal functions. Equally important is our commitment to transparency, which is why "The Bloomberg Way" is a public document.

As we've grown, and as data privacy has become a central concern to our clients, we should go above and beyond in protecting data, especially when we have even the appearance of impropriety. And that's why we've made these recent changes to what reporters can access.

This leads to a second point lost in much of this weekend's conversation: The protection of important customer data has been essential at Bloomberg since our founding more than 30 years ago. We have never compromised the integrity of that data in our reporting.

At no time did reporters have access to trading, portfolio, monitor, blotter or other related systems. Nor did they have access to clients' messages to one another. They couldn't see the stories that clients were reading or the securities clients might be looking at.

Like all other Bloomberg employees, our reporters, upon hiring, enter into a confidentiality agreement that strictly prohibits them from discussing non-public Bloomberg documents and proprietary information about the company and its clients in their reporting.

Our editorial and reporting standards have been among the most stringent in the business for more than 20 years. We apologize for our error as it does not reflect on our culture or our heritage. And we will strive to continue to uphold the highest standards while adhering to the best practices in the industry as long as we may be fortunate to serve our customers as they would have us serve them.

([Matthew Winkler](#) is the editor-in-chief of Bloomberg News. The opinions expressed are his own.)

Read Bloomberg chief executive officer Daniel L. Doctoroff's [statement on safeguarding customer data](#).

To contact the author of this article: Matthew Winkler at mwinkler@bloomberg.net.

To contact the editor responsible for this article: David Shipley at djshipley@bloomberg.net

Appendix F

Bloomberg's Client Data Principles

CLIENT DATA PRINCIPLES

Bloomberg clients rely on our unique financial solutions and exceptional customer service. These solutions and services require the thoughtful integration and analysis of client, third-party and proprietary Bloomberg information. Client trust is therefore our highest priority and the cornerstone of our business.

These Client Data Principles inform and guide decisions made throughout Bloomberg by our employees, contractors, and temporary staff (collectively, "Personnel") about data we collect from our clients and end users through their use of Bloomberg's products and services ("Client Data").

Respect: We handle Client Data in a manner respectful to our clients and end users. We constantly examine how our principles, policies and procedures help us provide the protection our clients deserve and we respond thoughtfully to their questions, opinions, and concerns.

Transparency: We communicate with clients about our policies for Client Data. Accurate and useful information about our Client Data practices is available through our products and services, Bloomberg.com, customer service, and other authoritative sources.

Personnel Access: We grant Personnel access to Client Data only as necessary for them to carry out their responsibilities. Such access is regularly reviewed and confirmed through our role based permissioning systems and procedures.

Security and Privacy: We invest in and maintain administrative, technical, and physical safeguards to protect Client Data. We engage in ongoing monitoring and testing of the efficacy of these safeguards.

Innovation: We constantly seek to create value for our clients through innovation, and we apply the same approach to our Client Data practices. By referencing relevant international security and privacy standards and building new solutions that anticipate the unique needs and concerns of our financial services, government, and corporate clients, we establish industry-leading practices.

Personal Accountability: All Bloomberg Personnel are personally accountable for acting consistently with these Principles and in accordance with relevant policies and procedures. We understand that there are consequences for behavior that is inconsistent with these Principles.

Governance: Senior management is responsible for strong and effective governance, including ensuring that we implement the letter and spirit of these Principles through policies, procedures, training, monitoring, testing, and auditing.