Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 31, ISSUE 22 / APRIL 10, 2014

EXPERT ANALYSIS

Trust and Transparency in the Era of 'Bring Your Own Device'

By Elizabeth E. McGinn, Esq., James T. Shreve, Esq., and Purvi S. Patel, Esq.,
BuckleySandler LLP

Information, including proprietary business information and personally identifiable information, is one of a financial institution's most precious assets, and protecting this asset is necessary to establishing and maintaining long-standing relationships between a financial institution and its customers. Moreover, the reputation and success of a financial institution are linked to its management and protection of sensitive information. The increasing prevalence of the BYOD trend — "bring your own device," in which employees use their personal mobile devices for work purposes — has drastically changed the rules of engagement when it comes to protecting a financial institution's information assets.[1]

Employees are undeniably using their personal mobile devices to access company data and systems, whether or not expressly permitted or regulated by the institution's corporate policies. These employees are simultaneously demanding greater flexibility and formal approval to use their mobile devices for work purposes. It is important that financial institutions take proactive steps to protect their information systems with the buy-in and support of their employees. Employees, however, are wary of allowing employers access and, in some cases, control over their personal mobile devices.

The ultimate goal of the institution, and its employees, is the protection of sensitive corporate information, with minimal intrusion into the personal data of employees. To achieve optimal results, both parties may be best served to acknowledge a shared responsibility that requires mutual trust and cooperation.

RESPONSIBILITIES OF FINANCIAL INSTITUTIONS

Financial institutions are bound by legal and regulatory requirements to adequately safeguard sensitive data, including providing proper oversight of the information security controls used to protect this data.[2] At the federal level, the financial regulatory agencies have issued requirements for financial institutions' information security controls. The Federal Trade Commission and the federal bank regulatory agencies issued final rules pursuant to Section 501(b) of the Gramm-Leach-Bliley Act establishing standards for financial institutions to adequately safeguard customer information. These rules include a requirement to develop a written information security program that "contains administrative, technical and physical safeguards" to protect sensitive customer financial information.[3]

In the Federal Financial Institutions Examination Council IT Examination Handbook, the joint regulatory body states, "Financial institutions should implement an ongoing security process and

institute appropriate governance for the security function, assigning clear and appropriate roles and responsibilities to the board of directors, management, and employees."[4]

Specifically, financial institutions have a responsibility to:

- Identify and assess threats and breaches of their data.
- Enact a plan to mitigate the risk of an information security breach.
- Implement adequate security controls and delegate responsibilities to managers and staff.
- Monitor and test the security controls to verify they are effective.
- Continuously update the existing controls to ensure they are current and adequate to deal with new threats and vulnerabilities.[5]

While the responsibility of maintaining and implementing effective information security controls rests with the institution, establishing trust between the institution and its employees is an important component in the success of the security process.

It is important that financial institutions take proactive steps to protect their information systems with the buy-in and support of their employees.

Additionally, one state in particular has adopted a comprehensive information security regulation that goes beyond the requirements issued by federal regulators, both in purpose and in scope.[6] In Massachusetts, any company or person possessing personal information relating to a state resident is required to adopt a written information security policy containing several safeguards for information and systems, including access control requirements, encryption for personal information sent across public networks or stored on portable devices, and systems monitoring. While the regulation adopted by Massachusetts technically governs only information relating to that state's residents, the regulation has become a de facto national standard for companies throughout the country.

RISKS FROM BYOD

Perhaps the biggest risk posed to a financial institution by the introduction and proliferation of the BYOD phenomenon is data loss. Data may be lost through manipulation of a lost or stolen device with inadequate security controls, or through employee carelessness or disobedience of company security policies, which can lead to malware attacks on their mobile devices, thereby putting sensitive corporate data at risk of disclosure. Studies conducted in 2012 and 2013 found that about 80 percent of U.S. companies surveyed permitted employees to use their own mobile devices at work.[7] In 2012, over "half of companies that permit BYOD reported experiencing a data or security breach as a result of an employee-owned device accessing the corporate network."[8]

Financial institutions are also susceptible targets for sophisticated hack attacks that have the capacity to shut down the institution's website, interrupt customers' access to their finances, and risk disclosure of customers' personally identifiable information and sensitive financial data.[9] Debilitating hack attacks that put regulated data, including information about customers, transactions or mergers, at risk of being leaked is further enhanced when employees are permitted to access confidential company data on personal devices that may be insecure and retain the capability to manipulate or even disable the security settings on their mobile devices.[10] As a result, financial institutions are well advised to engage in transparent and candid dialogues with employees to quell their concerns about unnecessary corporate intrusion into their personal mobile devices and to ensure that employees are aware of the risks to the company so they will take measures to protect company data on their devices.

COMPANY CONTROLS REQUIRED

The cornerstone of an effective BYOD policy that protects important company data and respects the privacy of employees is transparency and trust between the institution and its employees. A partnership between the institution and its employees requires both parties to be aware of the risks posed to each party and take appropriate actions to mitigate that risk.

The institution is concerned about losing access and control of company data, while employees are concerned about losing privacy of their personal data in their mobile devices. Thus, an important maxim of an effective BYOD policy is that an institution should clearly and effectively communicate to its employees the parameters of permissible uses of personal mobile devices, so that employees can make an informed decision about using their devices for work purposes.

Transparent communication about the rules and ramifications of BYOD will also encourage employees to proactively disclose an actual or potential breach of security to the institution so that both parties can work together to minimize information losses to the institution and to the employee.

A successful BYOD policy takes into account three important considerations. First, employees should be educated about how to keep company data safe and take proactive steps to ensure that company data is not compromised. Second, financial institutions may need to put clear limitations on employees' use of personal devices for work-related purposes. Finally, institutions may be best served by allowing employees a reasonable amount of control over personal information on their devices to the extent it does not compromise corporate data.

The ultimate goal of the institution, and its employees, is the protection of sensitive corporate information, with minimum intrusion into employees' personal data.

Proactive steps to protecting company data

Taking proactive steps to protect company data can prevent many incidents of improper system access and data exfiltration and make more efficient any remediation efforts to address incidents that occur. Thus, prudent risk management may dictate that a financial institution provide employees with a robust set of preventative controls that protect company data and the employees' devices.

Effectively communicating the responsibilities of employees in connection with BYOD is integral to maintaining a trusting relationship between the institution and its employees. As an initial matter, all employees who choose to use their own devices for company-related purposes should understand, agree to and follow a written BYOD policy.

Employees should be required to take preventive actions to secure their mobile devices through enforcing strong passcodes or PINs; installing antivirus protection, data loss prevention and auto-lock features; and encrypting data sent to and from the device.[11]

Employees may also be required to notify the IT and compliance departments in the event that their mobile devices are missing or stolen, and be prepared for the likelihood that their device will be geo-located and remotely wiped, removing all sensitive corporate data.[12]

Limits and restrictions on employees' use of personal devices

While regulatory agencies have yet to weigh in significantly on the topic, financial institutions are looking for guidance on how to appropriately limit their employees' use of personal devices for work purposes. The more transparently the institution communicates restrictions of BYOD, the fewer unintentional infractions it will face.

Some financial institutions allow employees to use their own devices for work purposes but require the installation of a firewall on the employee's device separating personal and company

information.[13] At one U.S. financial institution, employees are required to enroll their devices through a so-called mobile device management portal and agree to give some control of their devices to the company IT department.[14]

Financial institutions should also limit network points of access on a mobile device, so that an employee cannot view and access sensitive corporate data using an unsecured, untrusted wireless network. Finally, financial institutions should be wary of allowing employees to upload sensitive corporate data to public cloud-sharing services (such as Dropbox or Apple's iCloud) or access "core network resources" of the institution through their personal mobile devices.

Employees' control over personal data

The institution's interests in maintaining security of corporate data and the employee's interest in flexibility to work on a mobile device and maintain privacy of personal information are not mutually exclusive. Both parties can take steps to maximize efficiency, safety and privacy through an innovative written BYOD policy.

Perhaps most importantly, corporations can build trust with employees by listening to the concerns they have about maximizing efficiency but retaining privacy, and implement new solutions that do not compromise safety and security. First and foremost, corporations should recognize that effective procedures to address BYOD will ideally protect the privacy and security of employee data on the device.[15]

Financial institutions may be able to use certain technologies that limit BYOD risks and may, in some cases, limit potential disruptions to employees' use of their devices. Possible useful techniques and technologies include the following:

- "Sandboxing," a commonly used technique for mobile device management, is a containerization method that allows employees to isolate and "manage corporate data and run business apps [on their mobile devices] ... without having them intermingle with personal data."[16] Isolating virtual workspaces has the added benefit of permitting selective remote wiping of corporate data on a lost or stolen device, thereby protecting business assets while leaving personal data and settings intact.[17]

- A dual SIM card device eliminates the need for an employee to carry two devices, one for work and one for personal use, but permits the separation of communications and data through personal and work modes.[18]

- Private cloud sharing, which allows employees to access private clouds, as opposed to Dropbox or iCloud, appeases employees' desire for connectivity, allows them to be productive, and abates security and data leakage risks.[19] As an added bonus to the employee, cloud-based architecture also saves an employee's personal data if a device needs to be remotely wiped.[20]

- Corporate mobile applications let employees use their mobile devices to link to Sharepoint documents that allow communal editing features, and let an institution maintain security while giving employees additional flexibility to be productive and efficient.[21]

The technological potential of BYOD is far-reaching, and the use of mobile devices to access corporate data is certainly only the tip of the metaphorical iceberg. If employees are to continue to enhance their productivity while protecting sensitive corporate data, financial institutions may wish to be at the forefront of the BYOD movement.

CONCLUSION

BYOD is changing the way financial institutions manage and protect their most sensitive data. While the risks to information security have arguably exponentially increased because of the need to continuously monitor individual employees' actions and secure all mobile devices, the capacity for employee efficiency and satisfaction has also increased. The key to maintaining an effective, yet unobtrusive, BYOD program is contingent on the level of transparency and trust that is fostered and maintained between the institution and its employees.

A financial institution is tasked with educating its employees about the risks and benefits of BYOD and implementing appropriate basic controls to protect sensitive corporate data. However, institutions can also provide employees with active choices to safeguard their personal data and utilize technology to increase their productivity. The shared responsibility and mutual trust of both parties in implementing a BYOD program is integral to its overall success.

NOTES

[1] David Amerland, *BYOD: It's A Question of Lust (And Trust)*, Forbes, Oct. 17, 2012, http://www.forbes.com/sites/netapp/2012/10/17/byod-its-a-question-of-lust-and-trust/.

[2] Fed. Fin. Inst. Examination Council, Information Security IT Examination Handbook (July 2006); *see also* Fed. Trade Comm'n 16 CFR Part 314.

[3] Fed. Trade Comm'n, Standards for Safeguarding Customer Information; Final Rule. FTC, 16 CFR Part 314, 6 (2002), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf .

[4] *Id.* at 7.

[5] *Id.* at 7-8.

[6] Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.00: Mass. Gen. Laws ch. 93H, *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

[7] Cheryl Harris, Decisive Analytics, *Mobile Consumerization Trends & Perceptions: IT Executive and CEO Survey* (August 2012), *available at* http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_decisive-analytics-consumerization-surveys.pdf; *see also* Readwrite, *BYOD By the Numbers [Infographic]* (Mar. 26, 2013), *available at* http://readwrite.com/2013/03/26/intel-byod-by-the-numbers#awesm=~okxb0cxsFxFq7L/.

[8] Harris, *supra* note 7, at 4.

[9] Sean Martin, *Cyber Security Threat #3: Mobile Security Concerns*, Bank Innovation (Oct. 10, 2013), http://www.bankinnovation.net/2013/10/cyber-security-threat-3-mobile-security-concerns/; Carle Herberger, *How to Defend Against Hacktivists*, Bank Info Security (July 29, 2013), http://www.bankinfosecurity.com/how-to-defend-against-hacktivists-a-5948/; Penny Crosman, *Mobile Leaks Make Banks Wary of 'Bring Your Own Device' Trend*, Bank Technology News (July 1, 2013), *available at* http://www.americanbanker.com/issues/178_126/mobile-leaks-make-banks-wary-of-bring-your-own-device-trend-1060319-1.html/.

[10] *Id.* ("The study found that at 59 percent of companies, employees circumvent or disable required security settings on their mobile devices").

[11] Gerhard Eschelbeck, Sophos, *BYOD Risks and Rewards: How to keep employee smartphones, laptops, and tablets secure*, http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophosBYODrisksrewardswpna.pdf.

[12] MaaS360, *The Ten Commandments of BYOD*, http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf.

[13] Olivia LaBarre, *Banks May Not Be Able to Resist 'Bring Your Own Device'*, Bank Sys. & Tech. (Apr. 24, 2012), *available at* http://www.banktech.com/management-strategies/banks-may-not-be-able-to-resist-bring-yo/232900559/.

[14] Lisa Phifer, *BYOD security strategies: Balancing BOYD risks and rewards*, Search Security (Jan. 28, 2013), http://searchsecurity.techtarget.com/feature/BYOD-security-strategies-Balancing-BYOD-risks-and-rewards/.

[15] MaaS360, *supra* note 12.

[16] Sarah Fister Gale, *Creating a Secure 'Sandbox' on Employee Devices*, Workforce.com (Apr. 2, 2013), http://www.workforce.com/articles/creating-a-secure-sandbox-on-employee-devices/.

[17] Phifer, *supra* note 14; *see also* Eschelbeck, *supra* note 11.

[18] Kevin C. Tofel, *Why Samsung Just Entered the Dual-SIM Smartphone Game*, GIGAOM (Dec. 22, 2011), http://gigaom.com/2011/12/22/why-samsung-just-entered-the-dual-sim-smartphone-game/.

[19] Accellion Inc., *BYOD File Sharing – Go Private Cloud to Mitigate Data Risks*, *available at* http://resources.idgenterprise.com/original/AST-0090921_Accellion_WP_BYOD_File_Sharing_Private_Cloud.pdf.

[20] LaBarre, *supra* note 13.



Elizabeth E. McGinn (L) is a partner and **James T. Shreve** (C) and **Purvi S. Patel** (R) are associates at **BuckleySandler LLP** in New York and Washington. They advise financial institutions on privacy and cyber security compliance and represent financial institutions in litigation and investigations involving fair lending, financial fraud, privacy, and False Claims Act, FIRREA and white-collar criminal matters. They can be reached at emcginn@buckleysandler.com, jshreve@buckleysandler.com and ppatel@buckleysandler.com, respectively.