Locke Lord’s Data Protection Newsletter provides topical snapshots of recent developments in the fast-changing world of privacy and data security. For further information on any of the subjects covered in the newsletter, please contact one of the members of our data protection team.

Topics:

Page 2
HIPAA and Ebola Patient Privacy – OCR Weighs In

Page 3
Et tu, JPMorgan?

Page 4
EU Data Protection Supervisory Authority Issues Opinion on the “Internet of Things”

Page 5
U.S. Federal Communications Commission Enters Information Security and Data Breach Enforcement Territory

Page 6
Collaboration and Coverage – Insurance for Cyber Risks

Page 6
What’s in Store for Apple Pay?

Page 8
The “Poodle Bug”

Page 9
Guidance on the Proper Handling of Customers’ Personal Data for Hong Kong’s Banking Industry

Page 9
President Obama launches “BuySecure” Initiative with Executive Order
Topics: (cont)

Page 10
UK’s National Health Service Pilot Data Collection Scheme

Page 11
PCI DSS Compliance Reminder

Page 12
California Formally Requires Credit Monitoring, When Appropriate, for Data Breaches

Page 13
Amended CFPB Rule Allows Some Online Posting of Annual Privacy Notices
1. HIPAA and Ebola Patient Privacy – OCR Weighs In

A new bulletin published on November 10, 2014 by the U.S. Department of Health and Human Services (“HHS”), Offices for Civil Rights (“OCR”) reminds HIPAA covered entities and business associates that they must continue to safeguard protected health information (“PHI”) in accordance with HIPAA in the event of public health emergencies, including potential new Ebola outbreaks. OCR notes that “the protections of the Privacy Rule are not set aside during an emergency”; however, the bulletin highlights various provisions in the HIPAA Privacy Rule that permit certain types of disclosures and offers specific insight into how OCR expects covered entities and business associates to navigate the Privacy Rule during a public health emergency.

In light of OCR’s specific acknowledgement of privacy obligations in such emergencies, covered entities and business associates must carefully evaluate HIPAA obligations as part of their preparedness planning and emergency responses. This includes procedures for handling disclosures related to individuals exposed to, or potentially exposed to, the Ebola virus.

Reports to the Media and Public

Except in limited circumstances, affirmative reporting to the media or the public at large about an identifiable patient, or the disclosure to the public or media of specific information about treatment of an identifiable patient, may not be done without the patient’s written authorization. In the case of a hospital or other healthcare facility, reports about a particular patient should be limited to facility directory information to acknowledge an individual is a patient at the facility and provide basic information about the patient’s condition in general terms (e.g., critical orstable, deceased, or treated and released). Such reports are generally subject to the patient’s objection or requested restrictions or, if the patient is incapacitated, the facility must believe that the disclosure is in the best interest of the patient and is consistent with any prior expressed preferences of the patient.

Disclosures Permitted to Public Health Officials

The Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to PHI that is necessary to carry out their health mission. Accordingly, a covered entity may disclose to the CDC (or other local or state health authorities) PHI on an ongoing basis as needed to report all prior and prospective cases of patients exposed to or suspected or confirmed to have Ebola. Many state and local governments have directed hospitals and other health care providers who may have potential Ebola patients to report to their local health officials. A covered entity may rely on representations from a public health authority, like the CDC, or other public official that the requested information is the minimum necessary for the purpose. OCR also notes that disclosures of PHI can be made to a foreign government agency if done so in collaboration with a public health authority.
Disclosures to Potentially Exposed Individuals
The Privacy Rule permits a covered entity to notify persons at risk of contracting or spreading a disease or condition. Disclosures are also permissible for purposes of carrying out public health interventions or investigations. PHI may also be shared with anyone as necessary to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. Before making such disclosures, covered entities should carefully evaluate whether the threat qualifies as serious and imminent. A healthcare provider must also consider state health information privacy laws and their own applicable standards of ethical conduct before making such disclosures.

Disclosures to Friends and Family
The Privacy Rule permits a covered entity to share PHI with a patient’s family members, relatives, friends, or other persons identified by the patient as involved in the patient's care. A covered entity also may share information about a patient as necessary to identify, locate, and notify family members, guardians, or anyone else responsible for the patient's care, of the patient's location, general condition, or death. OCR notes that, when necessary, this may include notification to the police, the press, or public at large. Disclosure to disaster relief organizations, like the American Red Cross, may also be permissible. Under most circumstances, a covered entity should obtain verbal permission from the individual or otherwise be able to reasonably infer that the patient does not object to the disclosure.

Disclosures for Treatment Purposes
The Privacy Rule permits covered entities to disclose, without a patient’s authorization, PHI about the patient as necessary to treat the patient or to treat a different patient. Treatment can include coordination or management of health care and related services by one or more health care providers and others, consultation between providers, and referral of patients for treatment. Interestingly, in the bulletin, OCR interprets the definition of “treatment” to include use of PHI for treatment of a different patient.

Maintain Usual Business Practices
In the event of a public health emergency, covered entities and business associates must continue to implement reasonable safeguards to protect PHI against intentional or unintentional impermissible uses and disclosures and follow requirements of the HIPAA Security Rule. Disclosures to or by business associates should be made in accordance with the Privacy Rule and to the extent authorized by the parties’ business associate agreement. Furthermore, it is important to note that even if a disclosure is permissible, most circumstances require a covered entity or business associate to make reasonable efforts to limit the information disclosed to that which is the “minimum necessary” to accomplish the purpose. Therefore, covered entities and business associates should continue to apply their role-based access policies to limit access to PHI to only those workforce members who need it to carry out their duties. Covered entities and business associates may also be subject to more restrictive state privacy laws, including those tied to public health.

Under limited circumstances, the Secretary of HHS may waive certain requirements and enforcement actions under the HIPAA Privacy Rule. If the Secretary issues such waiver, it would only apply (1) in the emergency area and for the emergency period identified in the public health emergency declaration; (2) to hospitals that have instituted a disaster protocol; and (3) for up to 72 hours from
the time the hospital implements its disaster protocol. Without a formal waiver, covered entities
and business associates are expected to continue complying with HIPAA in the event of a public
health emergency.

2. *Et tu, JPMorgan?*

A massive security breach at the mega-bank, compromising data of 76 million
households and seven million small businesses, made headlines in October 2014,
sending shudders down the spines of all but those with nothing to lose.

What did the malfeasors get? According to JPMorgan’s SEC filing, only names, physical
addresses, and email addresses of customers were compromised. Thus, despite its jaw-dropping
size, the breach did not actually trigger any myriad U.S. data breach notification laws. They
require individuals and in many cases regulators to be notified in the event names in combination
with unencrypted and unredacted payment card numbers, account numbers, or other sensitive
personal information, and in the case of California, email addresses in combination with
passwords, may be compromised. Evidently, JPMorgan’s robust IT security infrastructure
caught its attackers before they were able to infiltrate deeper into its digital fortress and access
the real treasure – account numbers, passwords, and other data that may give direct access to
customer funds.

The hacked information is, nonetheless, valuable in that it can be used, by those so inclined, to
launch phishing schemes, or be combined with other information available on the black market to
form a more complete profile of a JPMorgan customer.

Coming on the heels of other recent mega-breaches at mega-corporations (Target and Home
Depot, both involving payment card data), the JPMorgan affair is a reminder of how insidious
data breaches have become and how under certain circumstances, statutory breach reporting
requirements are only a part of the calculus of what information about a security incident is
publicly announced.
3. EU Data Protection Supervisory Authority Issues Opinion on the “Internet of Things”

The Article 29 Working Party (“WP29”) has released an official Opinion highlighting privacy issues surrounding recent developments in the “Internet of Things” (IoT), reminding those concerned that the Data Protection Directive applies in full to the IoT and suggesting practical measures to ensure compliance.

The IoT refers to a proposed development of the Internet whereby “smart” devices and applications will communicate with each other electronically. At the latest WP29 meeting in September, current Internet privacy issues across Europe were heavily discussed and the group adopted an Opinion which focuses on three developments in particular:

- wearable computing – including watches and glasses, in which sensors are included to extend their functionalities;
- quantified self – including sleep trackers and other devices regularly carried by individuals to record information on habits and lifestyle; and
- home automation (“domotics”) – including motion sensors that detect and record when a user is at home and what his/her patterns of movement are.

Amongst the issues highlighted by the group in respect of the IoT were lack of user control or consent, security risks, and limitations on the possibility to remain anonymous. The Opinion helpfully sets out recommendations that data controllers of the IoT should take to ensure compliance with data protection laws.

WP29 also discussed the decision-making process that European data protection authorities should follow when deciding on cases involving search-engine takedown complaints, following the controversial ruling on the “right to be forgotten” by the Court of Justice of the European Union earlier this year. Further announcements from WP29 are expected later this year explaining the common criteria data protection authorities should consider when handling these sorts of complaints.

At the September meeting, the group also provided an update on the European data protection reform proposals, particularly in relation to the transfer of personal data to third countries, including the provisions on binding corporate rules and the territorial scope of the new proposed law. The reform proposals are still under discussion by the European Council.

On October 24, 2014 the Federal Communications Commission entered a Notice of Apparent Liability for Forfeiture (the “Notice”) against two communications service providers in connection with the communications service providers’ information security and breach notification practices, and proposed a forfeiture of $10 million. The Notice has been highlighted as the FCC’s first major action in information security enforcement.

The Notice arose from an incident wherein an investigative reporter was able to access personal information maintained by the communications service providers using common Internet searching techniques. The information accessed included names, addresses, dates of birth, Social Security numbers, and driver’s license and state identification card numbers – information that the service providers had received from individual applications to participate in a program providing telephony services to qualifying low-income consumers. The FCC pointed out in the Notice that, in addition to access obtained by the investigative reporter, evidence demonstrated that a number of IP addresses accessed the subject’s personal information from countries “often identified as hot spots for identity theft.”

Acting pursuant to its authority under Sections 201 and 222 of the Communications Act of 1934, the FCC found that the communications service providers had failed to properly protect personal information, failed to employ reasonable data security practices, engaged in “deceptive and misleading practices” by not adhering to privacy policy assurances, and engaged in “unjust and unreasonable practices” by not notifying customers of the data compromise.

Although the entirety of the Notice stands as a first-of-its-kind from the FCC, a couple of the FCC’s statements in the Notice warrant special attention for any communications service provider seeking to maintain appropriate security measures or properly execute responses to an information security incident. First, the FCC stated that “given the state of technology, we believe the lack of encryption clearly evidences the unjust and unreasonable nature of the [service providers’] data security practices.” A communications service provider should encrypt personal information where technically feasible (a sound practice in any event). More notably, the FCC flatly rejected the service providers’ arguments that they had provided information security incident notifications to the extent required by state laws, and found the service providers’ “notification of anything less than all potentially affected consumers unjust and unreasonable, in violation of Section 201(b) of [the Communications] Act.” Apparently, the FCC is not limited by the absence of a federal breach notification law – going forward, a communications service provider should be reluctant to limit breach notifications to only those individuals residing in states having black letter law requiring such notifications.
5. Collaboration and Coverage – Insurance for Cyber Risks
Cybersecurity commands our collective attention – from global political and financial leaders to each individual device user. High-profile stakeholders agree that cybersecurity undergirds our physical, digital and social infrastructures. Evaluation of cyber risks and solutions is paramount. And for private entities, assessment of insurance needs and products is a key part of risk management.

We recently participated in a roundtable of representatives from the business community and the Center for Cyber Conflict Studies at the Naval War College Foundation. The Center urges, facilitates and supports collaborative public-private partnerships to tackle cyber risks. According to the Center, cyber risks can affect information, financial assets, supply chains, property and more. The Center warns that “cybersecurity is critical to the stability of our economy, society and national security.”

These sentiments are echoed by former U.S. Secretary of Homeland Security and former Governor of Pennsylvania Tom Ridge who now heads Ridge Insurance Solutions. In his keynote address at the recent Advisen Cyber Risk Insights Conference in New York, Secretary Ridge cautioned that cyber risks have the “capability to cause catastrophic business and societal disruption.” His company, working with five syndicates at Lloyd’s, London, recognizes that no entity can prevent every possible cyber incursion and therefore wants to work with insureds on developing “total resiliency management.” Insurers must, according to Secretary Ridge, help their insureds “manage the risk before the risk manages them” and “understand the role cyber insurance must play in a comprehensive risk management portfolio.”

6. What’s in Store for Apple Pay?
Apple Pay will mainly be based on near field communication (“NFC”) and Touch ID technology. In addition, payment tokens will be created (as a replacement for the users’ credit or debit cards) and stored on a secure chip on the user’s smartphone. When a payment is made at a participating store, an NFC connection will be built between the user’s smartphone and the merchant’s POS terminal, allowing the token to be sent to the merchant’s network. The payment will then be authorized by the user through a fingerprint scan. The funds will eventually be credited to the merchant’s account after a successful validation by the issuer of the credit or debit card.
But how safe will your data be? Only a short while ago Apple’s iCloud was implicated when nude photos of celebrities were leaked online. Apple said its cloud servers themselves weren’t hacked, but it also admitted that “certain celebrity accounts were compromised.” On the Mac World Website, we discover this in the Apple Pay FAQs:

**What about privacy — can I be tracked if I pay using Apple Pay?**

Apparently not. Eddie Cue, Apple’s senior vice president of Internet Software and Services, insisted: “Security is at the core of Apple Pay; but so is privacy. We are not in the business of collecting your data.” (Was that a shot at Google?)

When you go to a shop, Apple doesn’t get to know what you bought, how much you paid for it, or any other personal details. The guy behind the counter doesn’t get to see your name or your credit card number — all of which are potential weak spots of the current system, under which cards are occasionally cloned and ripped off.

Therefore Apple is not using iCloud to store your credit card numbers at all. They are stored encrypted in a special highly secure spot on your phone: With Apple Pay, instead of using your actual credit and debit card numbers when you add your card, a unique Device Account Number (“DAN”) is assigned, encrypted and securely stored in the Secure Element, a dedicated chip in iPhone. These numbers are never stored on Apple servers.

Apple isn’t storing details about your purchases, except that Apple Pay does keep a list of your most recent purchases in the Passbook app, and Passbook does save some data to iCloud by default. It’s not clear if that data about your purchases will be stored on iCloud, but Apple isn’t collecting transaction details like your credit card.

So Apple is suggesting that they will not be collecting customer pay data nor will they be allowing merchants to access who is buying the goods. Does this in itself cause a problem? Depending on the type of goods being purchased some may be age restricted, by not letting the merchant see the data surely that will restrict the merchant from being able to verify the age of the purchaser. That said, the merchant should not be relying on a payment method to ascertain the age of its customers. There are many other sources of information a merchant can collect from a prospective customer.

Still, loyalty is the merchant’s killer app that drives sales and, ultimately, mobile payment’s adoption. But Apple Pay has a big problem standing between it and its ability to deliver on this critically important value proposition. Apple Pay’s tokenization scheme makes it impossible for merchants to match the token issued by the networks back to their customer profile. Most merchants use account numbers and customer name as the way they do that. The anonymised Payment Account Numbers (“PANs”) and DANs coming out of an Apple Pay transaction make that impossible. For loyalty programs to work, merchants have to know who’s buying stuff from them, so this could be a real problem for merchants unless they can build something alongside it to recognise their customers like a loyalty card – but doesn’t that defeat the object of removing the card from the transaction!

Under proposed EU laws on security of Internet payments the Apple Pay solution goes a long way to protecting transactions made with it. The Apple Pay solution is especially appealing in the U.S.
where “chip-and-PIN” is only just arriving and the majority of cards are still mag stripe only. Notably, the large data breaches we’ve heard about recently at Home Depot and Target would not be able to occur with Apple Pay transactions, because those transactions don’t produce reusable data.

In conclusion, it would appear that it is still the early days yet for Apple in the payments world but they are clearly looking to produce a secure payment solution making it safe and easy for customers to pay. The question marks are still over what is happening with the payment data if Apple is not storing it and the merchants can’t see it. There is also the question of how the merchants will react to the knock on effects to their loyalty programs as they will necessarily have to find a workaround. And finally there is the question of data privacy and what consents Apple will be getting even if the data is only stored on the phone and not the iCloud.

7. The “Poodle Bug”

The “Poodle Bug” is yet another serious security vulnerability discovered in widely-used software that makes browsing less safe. This discovery, which evidently has gone unnoticed for years, follows previous cyber threats Heartbleed and Shellshock earlier this year.

The “Poodle” – which stands for Padding Oracle On Downloaded Legacy Encryption – has been found in Secure Sockets Layer (SSL) 3.0 web encryption technology. SSL is used to encrypt and protect a user’s browsing session when using public Wi-Fi. Details of the Poodle bug have now been issued in a security advisory compiled by three Google engineers, Bodo Moller, Thai Duong, and Krzysztof Kotowicz.

The bug enables hackers to hijack their victim’s browsing session and potentially access personal online accounts, including email, online banking, or social networking accounts. The hacking process is described as “man-in-the-middle” attack, in which the hacker taps into the connection between users and servers, using the same public Wi-Fi.

The Guardian newspaper reports that, despite SSL technology being nearly 18 years old, SSL 3.0’s use is still widespread. A newer encryption technology, called Transport Layer Security, is immune. By comparison, Heartbleed, a bug that enabled hackers to steal data from servers, affected two-thirds of the Internet in April this year. Then, in September, the more serious Shellshock bug allowed hackers to hijack of millions of machines around the world, unnoticed.

Microsoft has advised that customers disable SSL 3.0 on Windows for servers and PCs. Mozilla reportedly plans to disable SSL 3.0 in the next version of its Firefox browser and Google has said it would remove support for the software over the next few months.
8. Guidance on the Proper Handling of Customers’ Personal Data for Hong Kong’s Banking Industry

With customer complaints relating to the collection, storage and use of personal data on the increase, Hong Kong’s Privacy Commissioner for Personal Data (PCPD) has issued a Guidance Note for Hong Kong’s banking industry on the proper handling of customers’ personal data.

The Privacy Commissioner for Personal Data, Allan Chiang, said, “We note from past complaint cases handled by us that the banking industry has long been among the top three private sector organisations being complained against. Furthermore, the number of complaints in relation to banking practices has been growing, with a total of 373 cases in 2013–14 against 198 cases in 2012–13 and 212 cases in 2011–12. Taking into consideration the large customer database maintained by the banking industry and the sensitive nature of the personal financial information involved, we consider it appropriate to publish the Guidance Note to promote and reinforce the banking industry’s compliance with the Ordinance in handling customers’ personal data.”

The Guidance Note covers data handling situations and issues of importance to the banking industry, including personal data minimization and retention, intra-group sharing, international data transfers, interfacing with law enforcement, use of personal data in debt collection and use of personal data in marketing, as well as e-banking and data subject access concerns. The Note provides good advice and a number of specific examples and case studies – useful and illuminating to privacy professionals in Hong Kong, and elsewhere.


On October 17, 2014, in conjunction with remarks made to the Consumer Financial Protection Bureau, President Obama launched the executive branch’s new “BuySecure” initiative and signed an Executive Order, titled “Improving the Cybersecurity of Consumer Financial Transactions.” These actions are designed to provide greater security for individuals’ financial information, particularly in the context of credit and debit cards.

The Executive Order directs executive departments and agencies to take significant (and swift) action to provide greater security for consumers interacting with the federal government. Executive departments and agencies must act “as soon as possible” to transition payment processing terminals to “employ enhanced security features, including chip-and-PIN technology.”
The Secretary of the Treasury is to take steps by January 1, 2015 to ensure that payment processing terminals acquired by agencies through the Department of the Treasury include hardware capable of supporting enhanced security features, and develop a plan for agencies to install enabling security software. Certain government-issued cards that lack enhanced security measures are to be replaced, and agencies with credit, debit and other payment card programs are to provide plans to the Office of Management and Budget by January 1, 2015 for ensuring their respective cards include enhanced security features. Furthermore, within 90 days of the Executive Order a plan is to be presented to the President “to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and effective identity proofing process.”

The Executive Order also requires certain actions be taken to “reduce the burden on consumers who have been victims of identity theft.” The Attorney General, in cooperation with the Secretary of Homeland Security, is to develop guidance for submissions concerning compromised credentials to the National Cyber-Forensics and Training Alliance’s Internet Fraud Alert System. The government is also supposed to enhance information available through the Federal Trade Commission’s Identity Theft web resource.

The BuySecure initiative and the Executive Order come near the end of a year in which information security incidents have made headlines, with major retailers suffering incidents that impacted millions of U.S. consumers. These events have caught the attention of not only the federal government but also a number of major retailers (including Home Depot, Walgreens, and Walmart), who will begin to roll out secure chip-and-PIN compatible card terminals. American Express is set to start a program to support upgrades to small business point-of-sale terminals.

With information security legislation currently tied up in Congress, actions like the Executive Order may represent U.S. companies’ and consumers’ best chance to dramatically improve information security for cardholders – like the 70% in-store fraud decline in the UK noted in the President’s remarks as a result of enhanced card and financial security systems.

10. UK’s National Health Service Pilot Data Collection Scheme

The UK’s National Health Service (“NHS”) has approved the creation of a patient database despite wide criticism by GPs and privacy issues raised by patients. The database will see the collection of personal data, including confidential medical information of 1.7 million patients by 265 GP surgeries across the UK.

The data-sharing scheme (costing £50 million) is designed to improve healthcare by advancing medical research and highlighting any instances of poor care. The scheme will involve personal data – which may include anything from past childhood illnesses to current medical conditions – being uploaded to the new database unless the patient actively opts-out.
The “Care.data” scheme was due to commence earlier this year but was delayed by strong opposition from senior GPs and privacy rights campaigners. One reason for the GPs’ strong opposition against the Care.data scheme was based on the requirement for patients to opt-out of the scheme rather than to opt-in. This requirement is still the case in the scheme’s current form and has caused much debate.

A campaign group, Patient Concern, has urged GPs that they “must automatically opt-out all their patients and then only remove that opt-out when patients give permission,” or else they risk undermining patient trust in their GPs. Dawn Monaghan, ICO public services strategic liaison group manager, has reportedly commented that this automatic opt-out strategy is not prevented by the UK Data Protection Act, but that it is ultimately an issue for the NHS to decide, so long as “patients are given a full explanation of the options open to them, and why the GP has chosen to opt them out.”

11. PCI DSS Compliance Reminder: Check Your Contracts! Deadline for Written Acknowledgements From Service Providers Is Fast-Approaching

Version 3.0 of the Payment Card Industry Data Security Standard (“PCI DSS”), which is now effective, will phase out PCI DSS version 2.0 at the end of this year, thus most of the requirements of Version 3.0 must be fully phased in by the start of 2015. PCI DSS version 3.0 contains several new requirements that are considered best practices until June 30, 2015, but thereafter will become required practice for any company subject to PCI DSS.

What requirements are changing?

All companies subject to PCI DSS will have to implement version 3.0 by January 1, 2015, with the exception of certain new technical / operational requirements, which will become mandatory on June 30, 2015. Notably, new requirement 12.9, which has a July 1, 2015 compliance date, will require that “Service providers [must] acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer’s cardholder data environment.” PCI DSS does not mandate any specific wording for this acknowledgement. Adding compliant language to all relevant contracts is likely to require lead time to negotiate the additional assurances with payment processors.

A “Service Provider” under PCI DSS is a business entity that is not a payment brand (VISA, MasterCard, American Express, etc.) that is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity, or that provides services that control or could impact the security of cardholder data. (Providers of public network access, such as telecommunications companies, are not considered a “Service Provider” for that service.)
What do I need to do to comply with the new requirements?

• Companies should adopt written procedures for screening and monitoring Service Providers before January 1, 2015.

• Companies should ensure that all vendors who must be PCI compliant are compliant with version 3.0 by January 1, 2015.

• Companies subject to the PCI DSS are required pursuant requirement 12.8.1 to maintain a list of Service Providers having access to cardholder data.

• Companies should review their relationships with all of their Service Providers who have access to cardholder data and who will need to provide a written acknowledgement pursuant to requirement 12.9. Companies should prepare written acknowledgements for delivery to Service Providers. Some Service Providers may be surprised by the new acknowledgement requirement, and others may push back, so adequate lead time should be provided to ensure timely compliance. Form agreements should also be carefully reviewed to ensure that the appropriate acknowledgement language is included on a going forward basis.

When must I comply with the new requirements?

PCI DSS v. 2.0 will remain active until December 31, 2014, and PCI DSS v. 3.0 will need to be fully phased in by January 1, 2015, other than several provisions, including requirement 12.9 noted above, that remain best practices until June 30, 2015.

12. California Formally Requires Credit Monitoring, When Appropriate, for Data Breaches

California has taken the lead once again in the privacy field by enacting a law that not only expands the state’s reach with respect to its current data protection and breach notification laws, but more importantly, now requires a business to offer, at no cost to an affected resident, “appropriate identity theft prevention and mitigation services, if any” after a breach of personal information.

California’s new law, AB 1710, can be found here. AB 1710 was enacted after a wave of recent breaches (e.g., Neiman Marcus, Target, and other retailers) left individuals vulnerable and unaware of available measures to adequately protect themselves in the aftermath. Assembly Floor Analysis from August 21, 2014, states the change to the law is “designed to improve security, enhance consumer notification, and limit consumer harms when a breach does occur.”

Historically, businesses offering identify theft prevention services after a breach were doing so voluntarily, with varying motivations driving the decision to offer. A business might fear a backlash from the public – including its customers – if it didn’t appear to be taking every precaution possible to assist the individuals. In addition, identity theft protection is offered out of a desire...
to mitigate damages. Credit monitoring may also have been offered because the regulators ask about it – indeed, some states have data breach notification forms that inquire whether a business offered identity theft prevention services. See, for example, New York’s form here. Before California, though, the states did not mandate that a business must offer such services to impacted individuals. As federal data breach bills continue to fail or remain bogged down in Congress, states may again follow California’s lead in data privacy, and enact laws that require and regulate offers of free identify theft prevention services upon a breach of personal information.

13. Amended CFPB Rule Allows Some Online Posting of Annual Privacy Notices

Some financial institutions may now provide annual privacy notices online, instead of sending them through the mail, thanks to a finalized amendment ("Amendment") released by the Consumer Financial Protection Bureau. The Amendment represents an effort by the CFPB to reduce costs associated with annual privacy notices that financial institutions must provide in accordance with the Gramm-Leach-Bliley Act ("GLBA") and CFPB Regulation P.

Financial institutions have, pursuant to the GLBA and Regulation P, annually mailed copies of notices to their customers setting forth basic information about how nonpublic personal information is collected and shared. These mailings present a significant cost and burden to financial institutions and, in a time when electronic information is increasingly more useful and easier to access and retain than paper documents, are of significantly diminished use to customers. Under the Amendment, which is now in effect, financial institutions subject to the CFPB’s jurisdiction may meet their annual GLBA notice requirements via online posting (along with several other practices designed to provide customers direction to find and understand the notice) if the following conditions are met:

- the financial institution does not disclose customers’ nonpublic personal information to nonaffiliated third parties, other than for specifically-allowed purposes;
- the financial institution does not include opt-out opportunities in the notice that are required in connection with certain information sharing practices pursuant to the Fair Credit Reporting Act;
- the notice is not the only means by which the financial institution satisfies requirements under the Fair Credit Reporting Act relating to sharing of nonpublic personal information between affiliates for marketing purposes;
- the financial institution is required to make only certain, permitted (if any) changes to its notice since having provided its immediately preceding notice (i.e., the financial institution has not changed its information collection and use practices in a manner that requires additional notification to customers); and
• the financial institution provides notice using one of several forms endorsed by the CFPB.

With respect to the second, third, and fourth bulleted requirements, above, it is notable that the CFPB has acknowledged a hope that these requirements will have a chilling effect on information sharing on the part of financial institutions by providing an incentive to reduce sharing that would preclude the advantageous permissions of the Amendment.

The Amendment was quickly met with criticism from industry and the legal community, who opined that it will do little to ease burdens for most financial institutions because of information-sharing-related limitations and will provide little benefit to consumers. These critics note that efforts pending before Congress may allow for online posting of privacy notices, but without conditions that would require financial institutions to choose between the burdens of annual mailings and the benefits of existing, non-extraordinary information sharing practices.