Thomas on Data Breach: A Practical Guide to Handling Data Breach Notifications Worldwide

By Liisa M. Thomas

2014

THOMSON REUTERS™

For Customer Assistance Call 1-800-328-4880

Mat #41648883

ISBN 978-0-314-63417-7

In loving memory of my mother, Melinda. A supporter and role model for us all.

About the Author

Liisa Thomas is a partner in the law firm of Winston & Strawn LLP and chair of the firm's global privacy and data security practice. Ms. Thomas has spent almost two decades helping clients with privacy law issues. Her clients rely on her to create clarity in a sea of confusing legal requirements, and for her down-to-earth delivery of efficient results.

Ms. Thomas, who was born in Finland and has lived in France, Egypt, and Spain, frequently coordinates global privacy efforts for her clients. Clients value her global insights and familiarity with business systems outside of the U.S.

Ms. Thomas has been recognized by the Leading Lawyers Network, *Chambers*, and *Legal 500*. She has been praised for her "superb advertising and privacy law practice" and her "encyclopedic mind." She is described as "remarkably perceptive [and] responsive," someone who "always consider[s the client's] business environment," and is praised for her ability to "explain issues and get to the heart of the matter."

Ms. Thomas is the editor of the firm's Privacy Law Corner blog, and is on the adjunct faculty and educational advisory board at the John Marshall Law School Center for Information Technology and Privacy Law. She received a B.A. in History from Haverford College and a J.D. from the University of Chicago Law School. She is an avid sailboat racer and plays violin in the Chicago Bar Association Symphony Orchestra, an orchestra made up of lawyers and judges. Ms. Thomas lives in Chicago with her husband and two sons.

Contributors

Monique Bhargava: Ms. Bhargava is a senior associate in the Chicago office of Winston & Strawn. Her practice includes counseling on consumer privacy law issues, including targeted advertising, mobile privacy, data security, and data breach response procedures. She received a BA in Political Science and Molecular Cell Biology with an emphasis in Neurobiology in 2004 from the University of California at Berkley. She received her JD, *magna cum laude*, in 2008 from the University of Illinois College of Law, where she was symposium editor of the *University of Illinois Law Review*.

Liz Brodzinski: Liz Brodzinski is an associate at Mudd Law Offices in Chicago, where her practice includes counseling clients on privacy and Internet matters. She received a B.S. in International Business from Saint Louis University in 2008, and a J.D. at DePaul University College of Law with a certificate in Intellectual Property in 2011, where she was the Lead Articles and Business editor of the *DePaul Journal of Art, Technology, And Intellectual Property Law*. Ms. Brodzinksi also served as a Law Student Assistant Editor for the American Bar Association's *Annual Review of Intellectual Property Law Developments*.

Robert Newman: Robert Newman is a senior associate in the Chicago office of Winston & Strawn. He regularly counsels clients on compliance with privacy and data security laws and regulations, including data breach matters, behavioral advertising, and mobile marketing. Mr. Newman received a B.A. from the University of Illinois at Urbana-Champaign in 2003. He received a J.D. and Intellectual Property Certificate from the Chicago-Kent College of Law in 2006. Mr. Newman serves as a chair of the American Bar Association's Internet and Privacy Subcommittee, and speaks on privacy matters on a regular basis.

Pavel Sternberg: Mr. Sternberg is a 2013 graduate of American University's Washington College of Law, where he graduated *cum laude*, and was a Note and Comment Editor on the *American University Law Review*. He has spent extensive time researching data breach preparation and response, and interned with the Federal Trade Commission, where he focused on privacy and data security issues, including information sharing, and consumer protection practices.

In 2008 he received his B.A. with honors in History and Political Science, along with a Certificate in Business, from the University of Wisconsin - Madison.

Marc Trachtenberg: Mr. Trachtenberg is a senior associate in the Chicago office of Winston & Strawn. His practice includes regular counseling on privacy law issues, including management of data breach notifications. Mr. Trachtenberg received a B.A. in Political Science in 1998 from the University of Michigan and a J.D., *magna cum laude*, in 2006 from DePaul University College of Law, where he was elected to the Order of the Coif. He is active in the legal community, serving on the Emerging Issues Committee of the International Trademark Association, the Board of Managers of the Intellectual Property Law Association of Chicago, and the Membership Committee of the ICANN Intellectual Property Constituency.

Acknowledgements

This book could not have happened without the help of my colleagues, many of whom worked with me on more breach notice projects than we care to count. It also would not have existed without those clients (you know who you are) with the hard questions, the "interesting" fact patterns, and the panicked business teams. It is my hope that this book is a tool—and a thank you—not only for them, but for all of you. And for everyone who read drafts of the manuscript, and provided your feedback, thank you!

Any list will be incomplete, but my particular thanks not just to the contributors, Monique Bhargava, Liz Budzinski, Rob Newman, Pasha Sternberg, and Marc Trachtenberg, but also to my colleagues who have joined me on the "data breach road," William O'Neill, Sheryl Falk, Steven Grimes, Kari Rollins, Sara Chubb, Caroline Hudson, Ryan Martin, Jen Miller, and Lucas Pendry, and to my partners Brian Heidelberger, Ron Rothstein, Anthony DiResta, Brian Fergemann, Mary Hutchings Reed, and Paul McGrady, for your support.

And to my team of supporters, Michelle Askew, Beth Fulkerson, Jenna Johnston, Stacey Keegan, Brenda Lang, Diana Laskaris, Katherine Licup, Marielle Lifshitz, Tina Kourasis, Cheryl Longstreet, Victoria Ocholla, Meg O'Hara, Joi Podgorny, Cynthia Van Ort, and Kathryn Woodward, you have made the practice of law a joy.

No acknowledgement could be complete without thanking my family: my husband whose patience knows (literally) no bounds, and my two lovely boys, Leo and Aaron. And a posthumous thanks to the one person in this world that made everything possible. My mother.

Preface

People have asked me why I decided to write this book. Perhaps I was bored? Or more likely, I had gone crazy? The former was definitely not the case. The latter—it all depends on who you ask.

I wrote this book because it did not exist. And I believed that it should. Those of us in the business of dealing with data breaches—whether as outside counsel, in-house attorneys, IT teams, investigators, or from another perspective—all know how frustrating breach notification laws can be. Just when you think you have memorized every possible requirement, a new one pops up.

And then comes that moment that you need to explain the process to senior leadership. We have to notify how many government authorities? By when? Really? Anyone who has undertaken a task like this knows just how daunting it is.

Yes, there are lots of freely available charts out there with lists of laws. Yes, there are lots of "super-secret" lists that those in this area have made over the years. Yes, there are lots of websites that tell you "if you have a breach, make sure to check the relevant laws." Yes, we all scour through these at top speed the minute we discover that a breach has occurred.

No, that is not good enough. With the many, many different laws and requirements that exist, waiting until the breach happens is hardly the right time to try to figure out what the laws are, what they require, and how you will analyze nuances.

Wouldn't it be helpful to have a tool that would help you do that? Even if you do wait until the last minute? (Because let's be realistic, most of you will wait until the last minute!).

I have always thought that my role as outside counsel was to help make people's lives easier. For each data breach project I work on with clients, that is my goal. Writing this, though, was my opportunity to do that on a much bigger scale.

This book is intended to fill a glaring void. If it is a helpful tool for you in the next data breach in which you are involved, I have succeeded. And if showing the book to your senior leadership to demonstrate how complicated this area is also helps, all the better. And even better still, what if government regulators read it and began to understand just

what a daunting—and expensive—task it can be to comply with all of these notice requirements? Requirements, that even if met, may not accomplish their stated goal of helping individuals protect themselves.

While I certainly did not anticipate it when I started this book almost a year ago, it is my hope that this book also helps with our national debate about data breach laws. Should there be more of these laws? Less? A universal federal law? More rapid notice? Deeper investigations by law enforcement? A stronger focus on data security rather than notification? As we debate these issues, this book can give us a comprehensive overview of where we are right now.

Although I think this book will be a helpful tool for you, I know that no book is ever done. That is doubly true of this one. This is the first edition, and there will be more changes in the law (hopefully not before this book goes to print!), more situations that practitioners will need interpreted, and more laws to discuss. If you think we should cover something that isn't included in this first edition, please let me know. This book is a tool for us all, and I hope that everyone will feel like they are a "contributor."

Please email me your comments, your requests for additions (to lmthomas@winston.com). Let's make this our joint work to attack the daunting task of global compliance with data breach notification laws.

Liisa Thomas
Chair, Privacy and Data Security Practice
Winston & Strawn LLP

Table of Contents

IV. DOES AN EXCEPTION APPLY?

CHAPTER 3. THE HEART OF THE MATTER: CONDUCTING INVESTIGATIONS

I. INTERNAL INVESTIGATION

II. COOPERATING WITH LAW ENFORCEMENT

II. NOTICE TO GOVERNMENT ENTITIES

III. NOTICE TO CREDIT REPORTING AGENCIES

IV. MISCELLANEOUS

APPENDICES

Chapter 1

Introduction

§ 1:1 The problem

There often is nothing worse, as a general counsel, than getting that call from your IT department: "we think our database of employee social security numbers was hacked." Or, "we think our online system has been compromised." Or, from HR: "a disgruntled employee just walked out the door with hundreds of social security numbers and is selling them on the black market." Or, the call from the FBI: "we think your company is under attack." Perhaps worse is being the one that has to make that call to the legal department or the CEO.

There is a flurry of activity. Teams will try to determine what information was accessed, who accessed it, and if employees or consumers have been put at risk. Each situation is fact-specific, so no amount of drills will answer these questions for every breach. Although the more breach-readiness drills a company does, hopefully the faster it gets at obtaining answers. If only because those at the company know what to ask.

Then there is the inevitable scramble to understand legal obligations. Do we have to notify under various data breach notification laws? Whom do we notify? How quickly? What should be included in the notice? What is our potential exposure after the notice goes out? And in the event of a

breach, the inevitable question: "did we do all that we could have to prevent the attack?"

§ 1:2 The law—A solution?

The answers to these questions can be tricky. Almost every state in the US has a data breach notification law. Some have two. There are also laws specific to those in certain industries. To say nothing of the growing number of breach notice laws outside of the US. Requirements to proactively protect information can further complicate the issue.

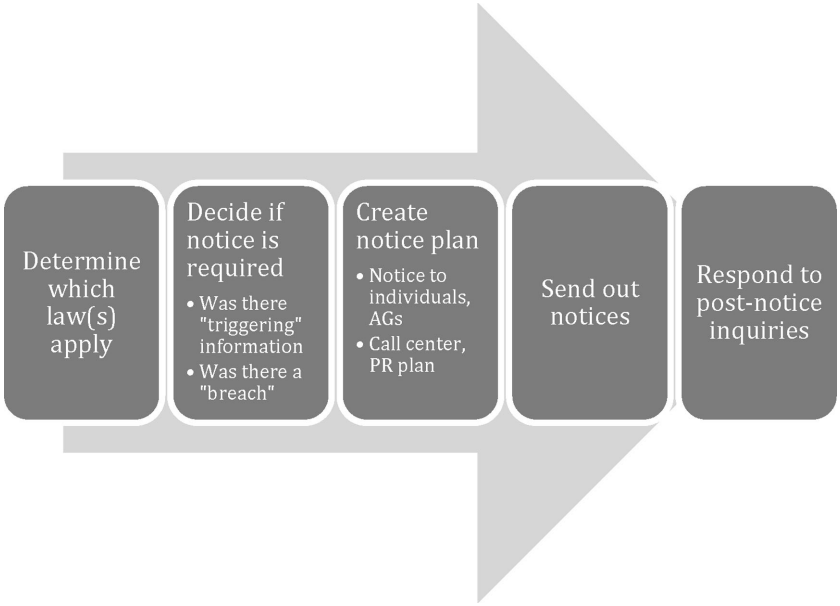
Then the already complex ramifications of a data breach can be exacerbated by class action exposure in the US, and the bad PR for the brand across the globe. That bad PR may result not only in falling stock prices, but possibly bigger hurdles from regulators looking at unrelated filings by the company. The company is tarnished in their eyes.

The general counsel that receives that call from IT or HR is understandably in a bad mood. And so is the person making the call.

How can we put everyone in a better mood? We can fully understand breach notification requirements, and have a clear plan in place before the breach occurs. And if the statistics are correct, the breach *will* occur. The websites of popular brands are constantly under attack by sophisticated hackers. It is often only a matter of time before they penetrate a company's defenses. To say nothing of the disgruntled or malicious employee, who decides that the road to riches is paved with stolen social security numbers.

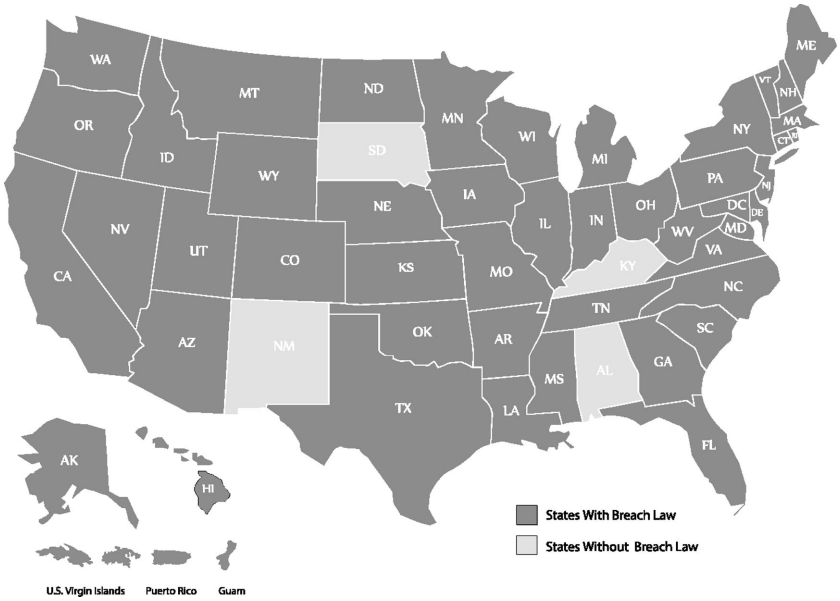
Where do we start? With a clear plan. We need to determine the scope of the breach notice obligations. What countries' laws apply? This will be based on an analysis of the impacted information, the location of the impacted individuals, and other fact-specific questions. We then look at the way those laws define "triggering" information such that the requirements would apply, and at the same time, whether the facts are such that a "breach" has indeed occurred. Once a determination is made to give notice, a notice plan will need to be put in place. This plan will take into account the need to notify impacted individuals, relevant government authorities, and potentially credit reporting agencies as well. Companies will need to think about how to get the notices out—and respond to potential inquiries. The notices will then go out, and finally, inquiries that come in will need responses.

Table 1-1 Breach Notice Process



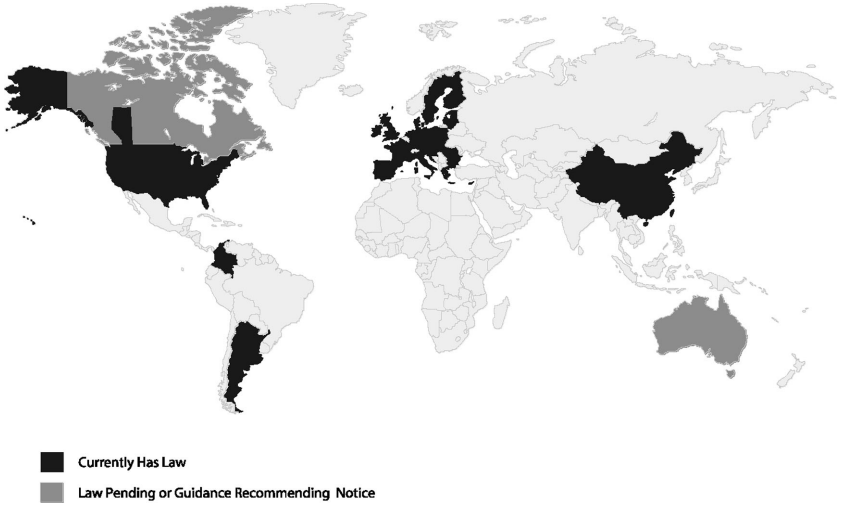
In the United States, most states and the District of Columbia have enacted data breach notification laws that require companies that own or license personal information to notify affected individuals in the event the company discovers or becomes aware of a breach of security involving certain types of information. And as mentioned, federal (and some state) laws exist that govern specific industries as well.

Table 1-2 US States with General Breach Notice Laws



Many other countries have some form of breach notice obligations as well. These include Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Colombia, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Ireland, Israel, Italy, Japan, Latvia, Lithuania, Luxemburg, Malta, Mexico, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Spain, Sweden, Switzerland and the United Kingdom.

Table 1-3 Breach Notice Countries



Even if a country does not have a specific breach notice law, there may still be an expectation—or perceived requirement—to notify impacted individuals. For example, in some locations, the view is that if information is used for a purpose that differs from the reason for which it was collected, the individual should be notified.

§ 1:3 Post-notice risks

If a business does not comply and fails to make the required notifications, it could face fines under these breach notice laws. And, in an unfortunate "catch-22," if a company does notify as required by breach notice laws, it opens itself up to potential suits under deceptive or unfairness statutes (for failure to adequately protect information, which failure it would be argued resulted in the breach). In the US, these suits might be brought by the FTC, state attorneys general, plaintiffs' class-action attorneys, or all three.

Even outside of the US, where class action lawsuits are less common, there is still risk associated with notice. This can often be in the form of damage to the brand image.

§ 1:4 How to get started

When determining if a breach has occurred, companies need to look at (1) which laws apply, (2) if the potential breach was of covered or "triggering" information, (3) if a "breach" has occurred as the term is defined under the relevant law(s), (4) how to go about conducting investigations,

(5) whether insurance coverage can pay for any of the process, (6) whether there are other reasons to notify absent a duty under breach laws, (7) if a breach has occurred, whom and how to notify, (8) what exposures exist and what steps can be taken to handle any post-notification fall-out, and finally (9) possible penalties for violating notice requirements.