CROWE&DUNLEVY
ATTORNEYS AND COUNSELORS AT LAW

Tips for Updating Your Cybersecurity Program and How to Handle Breaches

November 21, 2013

Anthony Hendricks, Associate
anthony.hendricks@crowedunlevy.com

Elizabeth Ann "Libby" Scott, Director
elizabeth.scott@crowedunlevy.com

Chair

Joe E. Edwards, Director
White Collar, Compliance and Investigation Practice Group Chair
joe.edwards@crowedunlevy.com

Members

Elliot Anderson, Associate
elliot.anderson@crowedunlevy.com

Daniel Burstein, Associate
daniel.burstein@crowedunlevy.com

Andre` Caldwell, Associate
andre.caldwell@crowedunlevy.com

Melanie Rughani, Associate
melanie.rughani@crowedunlevy.com

Jessica Perry, Associate
jessica.perry@crowedunlevy.com

Thomas Snyder, Director
thomas.snyder@crowedunlevy.com

In recent months, the federal government has placed growing attention on the importance of cybersecurity. In February, the White House issued an executive order on cybersecurity that focused on steps government agencies can take to protect critical infrastructures such as energy, defense and telecommunications.[1] However, more recently, attention has turned to financial institutions. While other critical infrastructures are subject to risk, financial organizations are the most hacked sector.[2] In 2012, almost 40 percent of all reported data breaches occurred at financial institutions.[3] A closer look at the data reflects the trend that cyberattacks continue to grow and, in particular, that smaller community banks are being targeted.[4] This is important news in Oklahoma because almost 60 percent of bank branches in the state are considered community banks.[5]

This summer, the Office of the Comptroller of the Currency (OCC) presented a webinar to community banks on cyberthreats, vulnerabilities and compliance programs. While most government agencies have largely been focusing on educating businesses of this risk, the Federal Trade Commission (FTC) has taken a different approach and started filing lawsuits against businesses for failures to protect customer data. For example, in 2010, the FTC brought suit against social media company Twitter for not providing adequate security of users' private information.[6] Similarly, in 2012, the FTC filed a complaint against Wyndham Hotel Group after the company suffered three hacker breaches over a two year span.[7] And this year, the FTC

1. The White House — Office of the Press Secretary, Executive Order: Improving Critical Infrastructure Cybersecurity, Feb. 12, 2013 (Cybersecurity Executive Order).
2. "2013 Data Breach Investigation Report, Verizon Enterprise," available at http://www.verizonenterprise.com/DBIR/2013/.
3. Id at p. 5.
4. "OCC Holds Web Conference for Community Banks on Cyber Threats" Office of Comptroller of Currency, June 12, 2013.
5. "Community Banks by the Numbers," FDIC Community Banking Research Project, Feb. 16, 2013 available at http://www.fdic.gov/news/conferences/communitybanking/community_banking_by_the_numbers_clean.pdf.
6. "Twitter Settles Charges that it Failed to Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program", FTC," June 24, 2010 available at http://www.ftc.gov/opa/2010/06/twitter.shtm.
7. A. Greenberg, "FTC Hits Wyndham Hotels With Lawsuit Over Three Hacker Breaches In Two Years," Forbes, June 26, 2012 available at http://www.forbes.com/sites/andygreenberg/2012/06/26/ftc-hits-wyndham-hotels-with-lawsuit-over-three-hacker-breaches-in-two-years.

brought an enforcement action against mobile phone company

HTC for, among other things, failing to protect user data and to train its employees on security risk.[8] While the FTC has not brought an action against a financial institution, these enforcement proceedings nevertheless stress the need for banks, especially community banks, to step up their efforts to protect themselves and their customers.

Because of community banks' size, unique role and increased targeting, these institutions have to take a different approach to protecting customers' personal information and responding to data breaches. Below are some helpful tips we offer community banks desiring to update their cybersecurity program, as well as three important steps to take if your institution or any business has been hacked:

Tips for updating your cybersecurity program

- **Know your risk**

Any compliance program should be risk based. For each bank, this risk is different. But there are some common themes. The first is that most breaches come from the outside.[9] So while controls on employees' access to customers' private information is important, there is a greater chance that it won't be an "inside job." A second common risk factor is the type of mobile access that is available to customers.[10] New technology like online banking, mobile phone access to accounts and deposits by phone makes banking more convenient for customers, but it also can expose banks to increased risk. Banks should examine the risks associated with each new innovation. Another risk factor is the nature of transactions done by the bank. These include the number, dollar volumes and the complexity. Finally, risk assessments should examine information systems, including network and software design, information processing, storage, transmission and disposal.[11]

- **Make your plan bigger than just technology**

When people think of protecting their information from hackers, they think of having the most sophisticated computer security software. But the most sophisticated program won't work if employees don't

8. "HTC America Settles FTC Charges It Failed to Secure Millions of Mobile Devices Shipped to Consumers", FTC, Feb. 22, 2013 available at http://www.ftc.gov/opa/2013/02/htc.shtm.
9. Verizon Enterprise,"2013 Data Breach Investigation Report."
10. "Mobile Banking Reward and Risk," FDIC Supervisory Insights - Winter 2011 available at http://www.fdic.gov/regulations/examinations/supervisory/insights/siwin11/mobile.html.
11. "Agreement containing Consent order," See In the Matter of HTC America available at http://ftc.gov/os/caselist/1223049/130222htcorder.pdf.

know how to use the program. Instead, technology should be seen as part of the solution but not the whole solution. Other parts of a compliance plan include employee training that addresses what to do when a worker gets a suspicious email or link; a policy that limits Internet surfing and downloading of programs on work computers; support from upper management stressing the importance of information security; and the designation of an employee or outside group to coordinate and be accountable for responding to problems. Banks should strive to create an environment where employees feel comfortable talking to their supervisor and the IT Department when they see something wrong with their computers without feeling embarrassed about their computer literacy skills.

- **Monitor and audit**

Once you have a plan in place, the work does not end. There must be regular testing or monitoring of the effectiveness of the plans, safeguards, systems and procedures implemented. Audits and tests should also identify new risks, updates in technology and changes in a bank's business practices. How often a bank conducts an audit should be based on the risk factors. For banks with a large number of risk factors, they should consider audits at least once a year, for medium risk banks every 12 to 24 months and up to 36 months for low risk banks. Auditing should be based on changes in risk. For example, reports by other banks of breaches, updates in your security software being released, the publication of new government guidelines, or the creation of new bank programs may each trigger an audit.

Tips for responding to cybersecurity breaches

While everyone hopes that their bank won't be a victim, it's important to have a plan if the unthinkable happens.

- **Don't panic…but take it seriously**

Data breaches can range from small viruses that affect one computer on a system to the type of full system attacks that are shown in spy movies. While each one may be treated differently, no matter the size, each of these should be taken seriously. When management treats all of these breaches as serious, it creates an environment of compliance. So no matter the scope of the problem, there should be a systematic effort to resolve the issue.

- **Let the IT department be the IT department**

Right after a breach, it's a natural reaction for people to want to solve the issue themselves. Don't do it. Report the problem and allow your

IT staff or information security team to get to work to determine what the issue is, what information is missing, if the risk is still ongoing and how to solve the problem.[12] Data breaches are crimes and you should think of your computer system as a crime scene. Don't tamper with the crime scene. You should also make sure that your IT department captures and preserves any data left by the hackers. They should also identify what went wrong so that you can make changes to your security plan.

- **Contact legal counsel**

If hackers have accessed customers' personal information, you may be under an obligation to inform your customers.[13] The state of Oklahoma, along with the Federal Deposit Insurance Corporation, has regulations on privacy and protecting consumers' private information. Attorneys with Crowe & Dunlevy's White Collar, Compliance and Investigations practice group can help you navigate your reporting requirements, create a compliance plan and update your plan after a security breach.

Contact:
Anthony Hendricks
405.239.5411
anthony.hendricks@crowedunlevy.com

Elizabeth Ann "Libby" Scott
405.234.3248
elizabeth.scott@crowedunlevy.com

About Crowe & Dunlevy

Crowe & Dunlevy, which has been providing effective legal counsel for over 100 years, is one of the most prominent law firms in Oklahoma, with offices in Oklahoma City, Tulsa and Norman. The firm and its attorneys are annually ranked among the top professionals in the nation by recognized peer-review organizations.

Oklahoma City
20 North Broadway
Suite 1800
Oklahoma City, OK 73102
405.235.7700

Tulsa
500 Kennedy Building
321 South Boston Avenue
Tulsa, OK 74103
918.592.9800

crowedunlevy.com

12. B. Worthen, "What to do when you've been hacked," The Wall Street Journal available Sept. 26, 2011 at http://online.wsj.com/news/articles/SB10001424053111904265504576566991567148576.
13. R. Richmond, "What to do if your Business get Hacked," Entrepreneur, December 4, 2011 available at http://www.entrepreneur.com/article/220807.