WEINER
BRODSKY
KIDER PC

Cybersecurity for the Mortgage Banking Industry

A Focus on Risks from Remote Work in the Coronavirus Crisis

WBK Webinar

April 23, 2020

Mitch Kider

kider@thewbkfirm.com

Michael Kieval

kieval@thewbkfirm.com

https://coronamortgagelaw.com/

Introduction

Data Security Is Always Important, but:

- Coronavirus increases the risks
  - More remote work
  - Information security risks inherent in remote work:
    - Shifts the balance of access vs security
    - Home networks vulnerable
    - Increased use of, proximity to personal devices
    - Harder to monitor individual behavior effectively
  - Increased vulnerability to social engineering attacks
  - Unique vulnerabilities if everyone is remote
    - IT (if you don’t have separate Infosec) may be focused on keeping everything working, unprecedented load
    - “Everyone's so isolated. No one really knows where anybody is.” -- Michigan AG Dana Nessel, quoted by CNN

WEINER BRODSKY KIDER PC

Introduction

Agenda:

- Regulatory Background
- What Regulators Are Saying
- What Is Happening
- What We Recommend
- Questions

WEINER
BRODSKY
KIDER PC

Regulatory Background

- Privacy laws
- Data protection laws
- Safeguards (data security) requirements
- Incident/breach notification requirements
- Business continuity/disaster recovery plans

Regulatory Background

- Privacy Laws
  - Govern what you can/cannot do with consumers', employees' data
  - *E.g.*, GLBA
- Data Protection Laws
  - Govern individuals' rights to limit/control even the permissible use of their own data
  - *E.g.*, GDPR, CCPA
- Privacy, data protection are always important
  - Remember to keep track of, comply with these requirements as you adapt to challenges

Regulatory Background

- Safeguards Requirements
  - These govern your (Written) Information Security Program
  - Regulations can be general or specific
  - FTC Safeguards Rule
    - Very general
    - Under GLBA
  - New York Cybersecurity Regulation
    - Broad application to entities licensed in New York
    - Detailed requirements for risk assessment and P&Ps
      - Details mostly left to companies, but some specific requirements
        - Focus on two-factor authentication
      - Must manage cybersecurity risk from third party service providers
  - Massachusetts
    - Somewhat general
    - Applies to any company with data of Mass. consumers

Regulatory Background

- Incident/Breach Response Plans
  - Are generally required by safeguards rules
  - Must also include notification, which is mostly state-law
- Breach Notifications
  - State laws define breaches differently
    - May require notice to:
      - Consumers
      - Data security regulators (AG or other regulator)
      - Credit reporting agencies
    - You will generally also give notice to your own licensing authorities
      - Even if the data breach law itself doesn't always require this
  - Unauthorized access to unencrypted data can be a "breach" even if not not hacked/not malicious in origin

Regulatory Background

Business Continuity/Disaster Recovery Plans

- You have one, presumably have implemented it
  - What have you learned?
  - Did it work as planned?
  - What didn’t you think of?
    - What can you learn about blindspots, ways to improve the plan?
  - How have you already changed it?
    - Formally or informally?
- Key issues:
  - Length of time, unanticipated limitations, vendors affected too, multiple locations affected simultaneously, consumers affected at same time

What Are Regulators Saying?

- FTC
  - Online security tips for working from home
  - Scammers are taking advantage of fears surrounding the Coronavirus
  - Warning of imposter scams (which can be particularly believable when things are chaotic)
  - Business scams (including the dangerous CEO/IT scam) are taking on a coronavirus flavor
  - Shortages can cause people to fall for a variation on supply scams using fake websites
- CFPB
  - Blog posts for consumers 3/27, 4/3 on scams
  - Warning 4/6 re: coronavirus mortgage relief scams
- FDIC
  - Consumer News March 2020
  - Warning on use of FDIC name in scams, fearmongering re: deposit insurance

What Are Regulators Saying?

- New York DFS
  - April 13, 2020 Industry Letter: Guidance re: Cybersecurity Awareness During COVID-19 Pandemic
    - Reminder that regulated entities must assess areas of heightened cybersecurity risk from coronavirus
    - Reminder that Cybersecurity Events must be reported w/in 72 hours – helps DFS monitor, respond to new threats
    - Heightened Risks of Remote Working
      - Make sure remote access is secure as possible, including MFA, VPNs for encryption in transit
      - Company-issued devices newly acquired or repurposed for remote work should be properly secured, including appropriate security software
      - BYOD expansion brings risks—companies should consider mitigating steps, compensating controls
      - Vulnerability of video and audio conferencing applications. Carefully configure, and provide guidance on secure usage
      - Shadow IT: Remind employees not to send NPI to personal accounts/devices.
        - “Anticipating and solving productivity problems will reduce the temptation to use such devices”

What Are Regulators Saying?

- New York DFS (cont’d)
  - April 13, 2020 Industry Letter (cont’d)
    - Increased Phishing and Fraud
      - Remind employees to be alert for phishing and fraud emails
      - Revisit phishing training and testing at earliest practical opportunity
      - Authentication protocols may need to be updated due to little face-to-face work
        - Especially for key actions like security exceptions, wire transfers
    - Third-Party Risk
      - Regulated entities should re-evaluate risks to critical vendors
        - Coordinate with critical vendors to determine if/how they are adequately addressing new risks
- CSBS
  - Examples of scams and warning signs
- Other States
  - California DBO
  - Washington DFI
  - Maryland Office of the Commissioner of Financial Regulation
  - Massachusetts Div. of Banks

What Are Regulators Saying?

- FinCEN
  - March 16, 2020: Encouraged financial institutions to remain alert to:
    - Imposter scams
    - Investment scams
    - Product scams
    - Insider trading
  - April 3, 2020: Guidance on implementing CARES Act:
    - Discussion of challenges with BSA compliance caused by crisis
    - Relaxing certain reporting obligations
    - COVID-19-specific online contact mechanism for financial institutions to communicate COVID-19-related concerns while adhering to BSA obligations.
- FHFA/GSEs
  - FHFA Coronavirus-Related Fraud Prevention Tips and Resources
  - Fannie Mae is linking to their general Beware of Scams page

What Are Regulators Saying?

- NACHA has delayed effective dates of its data security supplemental rule to 2021, 2022
- U.S. Secret Service warned of phishing increase
- FBI warned of rise in business email compromise schemes
  - Also exploitation of virtual work environments
  - Report online scams to FBI's Internet Crime Complaint Center
- DOJ runs National Center for Disaster Fraud
  - disaster@leo.gov or (866)720-5721

WEINER BRODSKY KIDER PC

What Has Been Happening?

Attacks are increasing:

- Phishing
- Wire transfer fraud
- Ransomware

What Has Been Happening?

Phishing

- Phishing is the use of social engineering to trick a user to click or provide info, to steal credentials or deliver malware
- Google says it blocks 18mm covid malware/phishing emails each day in Gmail (in addition to 240 mm covid-related spam messages)
- Phishing emails have been impersonating:
  - The CDC, with links to list of local coronavirus cases
  - Social Security, purporting to suspend benefits
  - Various government agencies, offering monetary relief
  - WHO/medical experts, with dangerous links/attachments
    - Variations of this appeared very early in other countries
    - Be especially wary of MS Office attachments

WEINER
BRODSKY
KIDER PC

What Has Been Happening?

Phishing (cont’d)

- Phishing emails have been impersonating (cont’d)
  - People in your company
    - HR, pushing out revised policies related to the crisis
    - IT/help desk
    - Senior executive sending tips to prevent infection
- Covid-19 contact scam
  - Text messages, with a link, saying you’ve come in contact with someone with coronavirus
- Fake apps
  - One app claimed to provide access to map with real-time tracking of coronavirus, was really a screen-lock attack

What Has Been Happening?

Phishing (cont'd)

- Some best practices to avoid email phishing include:
  - Automated systems to check/filter incoming emails
  - Firewalls and other defenses to prevent compromise even if a phishing email is received and a link or attachment opened
  - Educating employees on what to look for
    - Not to click on links or open attachments unless certain they're safe
    - Use real examples of realistic-looking emails that were not legitimate
    - Empower employees to think twice and say no
  - Make sure your business is run through processes that are regular enough that employees do not think that an ad hoc email is real
- To avoid phishing by telephone:
  - Have authentication processes in place
  - Train employees to spot social engineering, never make exceptions to authentication requirements

What Has Been Happening?

Wire transfer fraud

- Large payments in connection with real estate closings already make our industry susceptible to fraudulent wire instructions
- Common safeguards include calling for confirmation to known telephone numbers during business hours, not providing wire instructions by email, requiring written wire instructions in documents at outset of transaction, restrictions on changes unless in-person.
  - All of these are more challenging and/or less secure because of coronavirus
- Typical of business email compromise scams, which may be more believable now
- Reports of coronavirus being used as context for requests

WEINER BRODSKY KIDER PC

What Has Been Happening?

Wire transfer fraud (cont'd)

- In the current environment:
  - Do not allow last-minute changes or rushed wires
  - Authenticate any instructions that come by different means than usual. Consider using video if you know your counterparts well.
  - Make sure that people who are wiring money to you know that you have a single way of receiving wired funds and that you will not change it by email or telephone call
    - If you have to email wire instructions, consider instructing the recipient to call a known telephone number at the company to verify.
  - Consider instituting additional checklists for outgoing transfers, to confirm that the instructions are correct and the request is legitimate
  - If you are doing more electronic transfers where before a check would have been used, consider adding steps to slow down your process for those types of payments – take your time and double check
  - Look out for fraudulent requests related to HR/payroll and vendor payments (especially prepayment)

WEINER
BRODSKY
KIDER PC

What Has Been Happening?

Ransomware

- The stakes of keeping systems up and running are very high if you have to work remotely
  - Harder to recover or persevere with few people on-site
  - Client reliance on service providers increases pressure
- The increased susceptibility to phishing makes ransomware easier to implement
  - A number of the phishing attacks referenced above involved ransomware
- Even hospitals are not immune
  - Very high stakes, lots of other things on people’s minds

What Has Been Happening?

Ransomware (cont’d)

- The stakes are higher in the current environment, but the game is basically the same
- To protect yourself against ransomware:
  - Update and patch your systems and everything on them
  - Make and maintain backups of everything, at various points in time and in different places
    - Be conscious that newer ransomware tries to compromise your backups, too, before letting you know you’ve been attacked
  - Use antivirus software and firewalls, as well as behavior monitoring
    - Monitor and scan your systems for both suspicious files and suspicious activity
  - Limit the access/privileges that each user/account has to what that account needs.

WEINER
BRODSKY
KIDER PC

What Has Been Happening?

Other threats

- “Shadow IT”
  - When you don’t provide a workable solution, employees will find one
  - Risk at very beginning, before your solutions are rolled out, and later, as employees have time get creative
- Smart devices
  - Smart speakers: Amazon Echo/Alexa, Google Home/Google Assistant, Apple Homepod/Siri
  - Virtual assistants on cellphones and other devices
  - Video cameras inside homes
  - Any devices on home network add vulnerability
- Paper

What Has Been Happening?

Other threats (cont’d)

- Lack of physical privacy at home
  - Overheard conversations
  - Confidential information in video background
- Attacks on remote access/remote work infrastructure
  - Denial of service and ransomware attacks against service providers
  - Insecurity of remote conferencing facilities
    - *E.g.*, infiltration of Zoom meetings
    - Often tied to user-controlled settings or sharing of credentials

Try to distinguish between potential threats (which often make good clickbait) and significant trends

What Else Should You Be Doing?

- Strong firewalls and email filters are necessary
  - But not sufficient
    - Cybersecurity vendor Cofense posted a collection of phishing emails that evaded major platforms
- Training
  - Train staff to spot suspicious messages/requests
    - Always think twice
    - Don’t click links or open attachments, even in messages that look legitimate
  - It is better to miss a legitimate message than to click on a malicious one
  - Scams prey on sense of urgency – undo the urgency with process and give employees permission to pause.
  - Periodic reminders are important so people do not let their guard down

What Else Should You Be Doing?

- Multi-factor authentication
- Provide easy to use technology solutions
  - Employees will find ways to do their work—make sure you are in control
- Follow developments
  - From regulators, government agencies
  - From information security sources
- Limit access
- Monitor behavior
- Update, patch, and get rid of unnecessary points of entry

What Else Should You Be Doing?

- Continue to improve and adapt
  - Information security isn’t a one-time checkbox
  - You did your best under pressure at the beginning
  - Take the opportunity now to keep improving your defenses, stay one step ahead
  - Multi-layered defense is a must
- Also, don’t overpromise – regulators have brought enforcement for information security misrepresentations to consumers
- And most importantly, keep learning and improving to stay one step ahead.

WEINER BRODSKY KIDER PC

What Else Should You Be Doing?

- There are plenty of checklists and lists of best practices available for information security, from vendors, industry groups, government agencies
  - Use them
  - If you haven’t recently, run through the FFIEC’s toolkit
- But checklists aren’t enough
- What we have tried to do today is give you a way of thinking about the changes to the usual information security approach that are warranted by recent events
  - The approach is still sound, the tools are still the same
  - But the balances and trade-offs, the ways things work in practice, the details of implementation – all that has changed
  - By seeing and understanding those changes, you can adapt

Questions

?

WEINER
BRODSKY
KIDER PC

Cybersecurity for the Mortgage Banking Industry

A Focus on Risks from Remote Work in the Coronavirus Crisis

WBK Webinar

April 23, 2020

Mitch Kider

kider@thewbkfirm.com

Michael Kieval

kieval@thewbkfirm.com

https://coronamortgagelaw.com/