Law360

Data Security Best Practices For Licensed Lenders' Telework

By Sherry-Maria Safchuk, James Chou, and Frida Alim (September 1, 2020)

Sherry-Maria Safchuk

James Chou

Frida Alim

State-licensed/registered brokers, lenders and servicers have increased their focus on data security as the spread of COVID-19 has extended work-from-home orders, and what now seems to be a lasting acceptance of remote work means that the tools used to secure data will remain relevant when the pandemic ebbs.

This article examines recent state guidance on remote work and data security, highlights key data security requirements in recently enacted legislation, and identifies best practices for licensees to optimize or expand their remote working environments in a secure manner.

State Guidance Regarding Remote Work Highlights Concern Over Data Security

Broad concerns about the security of consumer data have pushed more than 40 state regulators to issue pandemic-related guidance on data security requirements for employees of licensees working from home. Some states, such as Arkansas[1] and Florida,[2] refer generally to existing state and federal requirements, while other states have set forth specific steps that licensees must take before employees may engage in remote work.

For example, regulatory guidance in California and Iowa permits employees of licensees to work from home only if employees use encrypted computers and devices and access the company's network using an encrypted virtual private network.[3] The Michigan Department of Insurance and Financial Services requested information from licensees and registrants regarding the measures taken to ensure the security of data and consumer information held offsite or transmitted to or from an offsite location.[4]

Companies should continue to monitor guidance from the states where they are licensed to determine whether specific requirements or reporting obligations apply.

Legislatures and Regulators Continue to Focus on Data Security

New legislation, including the New York Stop Hacks and Improve Electronic Data Security, or SHIELD, Act and the California Consumer Privacy Act, carry significant data security implications.[5] The Federal Trade Commission also has proposed significant changes to the Gramm-Leach-Bliley Act's Safeguards Rule that would impose specific requirements for information security programs similar to those under the New York Department of Financial Services Cybersecurity Regulation.

All 50 states now have data breach laws, and several in the past year have strengthened theirs, including by expanding the definition of "personal information," creating a private right of action for data breaches, or imposing deadlines for notifying consumers and/or regulators of an actual or suspected breach.[6]

For example, Massachusetts' data breach notification law requires organizations that experience a breach to also notify the relevant regulators as to whether the organization has a written information security program and the steps, if any, the organization has taken to update the program in response to an incident.[7]

State attorneys general also have taken an increasing role in policing privacy violations, underscoring the need for financial institutions to ensure robust privacy practices. In April 2020, the Massachusetts attorney general reached a settlement with Equifax Inc., a consumer credit reporting agency, for a data breach affecting 147 million consumers, resulting in a penalty of over $18 million.[8]

State attorneys general have also signaled that they will band together to investigate violations and enforce privacy laws, as evidenced by state AG coalitions that have been formed over the past year to investigate privacy concerns at major technology companies.

Similarly, the FTC has been active in addressing consumer privacy and, since 2002, has brought more than 70 cases against companies relating to the inadequate protection of consumers' personal data.[9]

In 2019, the FTC, along with the Consumer Financial Protection Bureau and 50 U.S. states and territories, reached a settlement with Equifax for over $575 million stemming from the above-mentioned data breach. The FTC required Equifax to impose a comprehensive information security program, as detailed in the settlement, and to obtain third-party assessments of its information security program every two years.[10]

The FTC also has stated that it is working closely with federal and state regulators, consumer advocates, and the business community to address unfair and deceptive business practices, which have historically included privacy violations, during the COVID-19 pandemic.[11]

Best Practices for Remote Work Environments

Licensees had been, for the most part, prohibited from conducting loan activities from an unlicensed location such as an offsite setting or home, but that changed with the pandemic.

Licensees should aim to maintain business continuity by leveraging as many rapid (but temporary) information security and data protection solutions to meet regulatory requirements that are both scalable and flexible to their needs.[12] At a high level, licensees should continue to:

- Review applicable data protection regulatory requirements and ensure that internal or third-party technology solutions address and comply with those requirements.

- Leverage, to the maximum extent possible in accordance with the institution's third-party risk tolerance, third-party cloud and technology platforms that could assist in providing secure remote work technology solutions.

- Review and update information security and data protection policies to consider remote operations, and communicate such updates to remote employees.

Review Information Security Requirements

As the privacy and information security landscape evolves rapidly, licensees should review information security program requirements and best practices. In addition to federal requirements, many state regulators have recently established specific information security standards to include:

- Multifactor authentication in a remote environment for users connecting from external networks;

- Encryption for data or communications in transit and for mobile devices containing sensitive information at rest;

- Least privilege principles, which provide that access to sensitive information should continue to be given only to select individual employees, contractors, or vendors;

- Passwords that meet certain requirements; and

- Incident response programs to respond to data breaches and other data security incidents.

Leveraging Third-Party Solutions

Many third-party providers, such as cloud service providers that bundle VPNs and virtualized desktop solutions, can provide critical technology solutions for licensees by emphasizing rapid deployment, scalability, flexibility and security without the need for licensees to reconfigure their internal networks. In selecting providers, licensees should consider the following information security guidelines:

- Access control: Does the provider empower the licensee to control access at the user level, use enhanced security options such as multifactor authentication (with replay resistance), grant and deny permissions at the user level, and, by default, deny access to any user that does not have explicit privileges to access the data?

- Secure communications: Does the provider offer reasonable assurances for the confidentiality of communications by using strong encryption?

- Network monitoring and data loss prevention: Does the provider enable the licensee to implement automated controls for monitoring network traffic, user access and data loss?

- Data integrity: Does the provider offer reasonable assurance that data hosted in its cloud would not be altered, destroyed or mishandled, either at rest or in transit?

- Established policies for vulnerability assessments, risk management and incident response: Does the provider have established policies, procedures, and standards to conduct vulnerability and risk assessments and to update its cloud platform upon the discovery of new or emerging vulnerabilities and maintain an executable incident response plan?

- Availability of platform: Does the provider have sufficient redundancy so that the licensee will have continuous access to its data and systems?

- Awareness of financial regulatory requirements: Does the provider have a history of experience with financial institutions and the data security and data privacy requirements unique to financial institutions?

Reliance on providers during a crisis may pose third-party risk challenges to organizations that have not previously considered remote operations, but there are several ways to mitigate this gap, such as:

- Requiring accreditation by a third party on certain aspects of the provider's platform, including the platform's assurances regarding availability, confidentiality, and integrity;

- Imposing requirements through contractual provisions, such as audit rights, mandatory compliance with applicable law, disaster recovery support, and service level objectives; and

- Performing due diligence on a provider's overall information security posture.

Cybersecurity Hygiene: Reviewing Policies Against Regulatory Requirements

Conducting a comprehensive review of an institution's written information security programs and applicable policies, procedures, and standards to incorporate remote operations is crucial as remote work may be here to stay in the long term. Not only is routine policy review and risk assessment consistent with regulatory expectations, but it can also help organizations achieve efficiency in planning and execution of cybersecurity solutions. A few policies to review include:

- Inventory and classification: Institutions should account for remote devices, user-owned devices and data residing outside the internal network, and establish procedures to discover and document such devices and data.

- Business continuity and disaster recovery: Business continuity and disaster recovery plans should be updated to include limited remote operations as a contingency, including any new service providers that will support the licensee's backup, recovery and remote operations.

- Logging and monitoring: To maintain accountability, security and data protection, institutions should consider remote monitoring or other logging activities as necessary.

- Authentication: Password, access and other authentication policies should be reviewed to ensure that strong passwords, multifactor authentication, and other enhanced authentication standards are implemented as necessary and where possible.

- Remote access, mobile device management, and noncompany-issued devices: Policies for remote access (i.e., access to the licensee's network through an external network) should be established and include guidelines regarding unsecured Wi-Fi use, storage of licensee data offsite or on a noncompany-issued device, and baseline configurations for mobile devices, such as antivirus software.

- Incident response: Since incidents, such as data breaches, may now occur remotely, incident response procedures should be updated to address breaches in remote environments.

- Vulnerability management and resilience training: Many breaches are caused by phishing or employee negligence, so awareness training should be a central part in all relevant environments.

Service providers offer good solutions for information security, but institutions must carefully assess the institution's compliance requirements, and any requirements applicable to service providers, and take reasonable measures to ensure the services acquired to assist with cybersecurity will meet regulatory requirements in the environments that the licensee operates.

Sherry-Maria Safchuk is counsel, and James Chou and Frida Alim are associates, at Buckley LLP.

[1] See, e.g., Ark. Securities Dep't, Extension of Interim Regulatory Guidance to Licensed Mortgage Companies, Mortgage Loan Officers, and Branch Managers (May 22, 2020), http://securities.arkansas.gov/!userfiles/Extension%20Interim%20Guidance%20for%20Mortgage%20Loan%20Officers%20May%202020.pdf.

[2] Florida Office of Fin. Reg., Guidance to Consumer Finance Industries (Mar. 20, 2020), https://dropinblog.com/uploaded/blogs/34235702/files/CF_Guidance_Final_32020.pdf.

[3] Cal. Dep't of Bus. Oversight, Guidance to Escrow Agents, Finance Lenders and Servicers, Student Loan Servicers, Residential Mortgage Lenders and Servicers, and Mortgage Loan Originators (Mar. 21, 2020), https://mortgage.nationwidelicensingsystem.org/NMLS%20Document%20Library/CA-DBO%20Guidance%20-%20Escrow%20Mortgage%20Student%20Loans%203.21.20%20-%20Coronavirus.pdf; Iowa Dep't of Banking, Regulatory Guidance for Working from Residence or Other Company Designated Location (Mar. 18, 2020), https://mortgage.nationwidelicensingsystem.org/NMLS%20Document%20Library/IA%20Guidance%20for%20Working%20Remotely%20-%20Coronavirus.pdf; see also District of Columbia Dep't of Insurance, Securities, and Banking, Order in Response to COVID-19 Public Health Emergency (Mar. 27, 2020, https://mortgage.nationwidelicensingsystem.org/NMLS%20Document%20Library/DC%20COVID-19%20Combined-Emergency-Order-Banking-MLOs-and-Foreclosure-Mediation-3-27-2020.pdf.

[4] Michigan Dep't of Fin. Servs., Letter to Consumer Finance Licensees and Registrants, https://www.michigan.gov/documents/difs/OCF_Survey_684276_7.pdf.

[5] Cal. Civ. Code § 1798.150(a)(1); see, e.g., Barnes v. Hanna Andersson, LLC., Case No. 20-cv-00812 (N.D. Cal Feb. 3, 2020); Henry v. Zoom Video Communications, Case No. 20-cv-02691 (N.D. Cal. Apr. 17, 2020).

[6] See, e.g., Arizona, S.B. 1614 (2d Reg. Sess. 2020); Connecticut, S.B. 134 (Feb. Sess.

2020); Connecticut, S.B. 137 (Feb. Sess. 2020); N.Y. Gen. Bus. Law §§ 899-aa, 899-bb.

[7] Mass. Gen. Laws Ann. ch. 93H, § 3(b).

[8] See Massachusetts v. Equifax, Inc., Civil Action No. 1784-CV-3009BLS2 (Complaint Mar. 31, 2020), https://www.mass.gov/doc/equifax-consent-judgment/download.

[9] FTC, Privacy and Data Security Update: 2019 at 5 (2020), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2019/2019-privacy-data-security-report-508.pdf.

[10] See FTC v. Equifax, Inc., Case No. 1:19-cv-03297-TWT (Complaint July 23, 2019), available at https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_order_signed_7-23-19.pdf.

[11] FTC, Statement from FTC Chairman Joe Simons Regarding Consumer Protection (Mar. 26, 2020), https://www.ftc.gov/system/files/documents/public_statements/1569773/final_chairman_covid_statement_3262020.pdf.

[12] Organizations interested in in-depth technical guidance may consider consulting the Federal Financial Institutions Examination Council's Interagency Statement on Pandemic Planning and the National Institute of Standards Technology's March 2020 ITL Bulletin and Special Publication 800-45. Fed. Fin. Inst. Examination Council, Interagency Statement on Pandemic Planning, https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf. See also Nat'l Inst. of Standards and Technology, ITL Bulletin March 2020: Security for Enterprise Telework, Remote Access, and Bring Your Own Device Solutions (Mar. 2020), https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf; Nat'l Inst. of Standards and Technology, NIST Special Publication 800-46 (Rev. 2): Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security (July 2016), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.