Stewart – Massachusetts Mid-Week Update – December 2, 2020

Dear Stewart Partners,

We have entered the last month of 2020! As we all reflect on the past 11 months, it is safe to say it was filled with unexpected challenges along with a boom in business, particularly in the residential sector with interest rates remaining at historic lows. Last week, apart from the Mid-Week update we shared the SJC's decision with you on the Thompson case, but have a further development to share in this week's update. Specifically, the borrowers in the case, the Thompsons, have filed a motion with the SJC for reconsideration.

In addition to the Thompson motion, in this week's update, we wanted to focus on cyber-crime awareness and prevention in business as well as vigilance away from the office. The holiday season generally sees an uptick in cybercrime in businesses and on individuals, particularly with the increased on-line and in-store shopping. We hope you find the following awareness tips and guidance helpful.

- **CASE UPDATE* The Thompson Motion – Appellees' Move for Reconsideration or Modification*

  Last week, the Supreme Judicial Court issued its ruling in *Thompson v. JP Morgan Chase Bank, N.A.* The Court determined that the Bank's statutorily required notice was not potentially deceptive and thus did not cause the foreclosure to fail. On November 30, the Thompsons filed their motion for reconsideration. We will continue to monitor the developments in the case and the outcome of the Motion for Reconsideration.

- *Cybersecurity Tips for Holiday Shopping from KnowBe4.com*

  For most of us, the holiday season is about friends, family, food—and shopping!
  Follow these tips to stay safe this holiday season:

  1. Keep your smartphone, computer, and other devices updated. This helps ensure that your device has the latest security patches.
  2. Only use trusted Wi-Fi connections and be suspicious of any network that does not require a password to connect.
  3. Take the time to change any outdated or simple passwords. Use strong, unique passwords on all of your accounts.
  4. Be careful not to overshare on social media. Consider anything you post to be public information.
  5. Keep an eye on the activity in your banking and credit card accounts. Also, be sure to monitor your credit report on a regular basis.
  6. Be suspicious of emails you receive about online purchases. Check the status of your order directly on the website that you purchased from.
  7. If you receive a holiday greeting card in your inbox, verify the sender before clicking the link to view the card.
  8. If you're traveling for the holidays, be sure to keep your devices stored safely at all times.
  9. Pay close attention to the websites that you order from. Only shop on websites that you know and trust.
  10. Watch out for giveaways and contests. Remember that if something seems too good to be true, it probably is.

- *Tips for Secure Video Conferencing*

In October, the American Land Title Association published an article providing guidelines and tips around secure video conferencing. These guidelines were established by The U.S. Cybersecurity and Infrastructure Security Agency (CISA) for individuals and organizations to enhance video conference security.

Connect Securely

The initial settings for home Wi-Fi networks and many video conferencing tools are not secure by default, which—if not changed—can allow malicious actors to compromise sensitive data while you work from home, according to CISA. Here are some quick tips to ensure a secure connection:

- Change default passwords to strong, complex passwords for your router and Wi-Fi network.
- Choose a generic name for your home Wi-Fi network to help mask who the network belongs to, or its equipment manufacturer.
- Ensure your home router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum, and that legacy protocols such as WEP and WPA are disabled.
- Avoid using public hotspots and networks.
- Only use video conferencing tools approved by your organization for business use.
- Enable security and encryption settings on video conferencing tools; these features are not always enabled by default.

Control Access

CISA says uncontrolled access to conversations may result in disruption or compromise of your conversations, and exposure of sensitive information. To mitigate this risk, companies should check their tool's security and privacy settings, and enable features that allow control of who can access video chats and conference calls. When sharing invitations to calls, ensure that you are only inviting the intended attendees. Here are additional tips from CISA to help control access to conversations:

- Require an access code or password to enter the event. Try not to repeat codes or passwords.
- Manage policies to ensure only members from your organization or desired group can attend. Be cautious of widely disseminating invitations.
- Enable "waiting room" features to see and vet attendees attempting to access your event before granting access.
- Lock the event once all intended attendees have joined.
- Ensure that you can manually admit and remove attendees (and know how to expeditiously remove unwanted attendees) if opening the event to the public. Be mindful of how (and to whom) you disseminate invitation links.

Manage File and Screen Sharing, and Recordings

CISA says mismanaged file sharing, screen sharing, and meeting recording can result in unauthorized access to sensitive information. Uncontrolled file sharing can inadvertently lead to users executing and clicking malicious files and links, which could, in turn, lead to system compromise. To alleviate this potential problem, CISA recommends disabling or limiting screen and file sharing to ensure only trusted sources have the capability to share. Users should be aware of sharing individual applications versus full screens. Here are some simple tips for controlling file and screen sharing:

- Toggle settings to limit the types of files that can be shared (e.g., not allowing .exe files).

- When recording meetings, make sure participants are aware and that the meeting owner knows how to access and secure the recording. Consider saving locally rather than in the cloud. Change default file names when saving recordings. Consult with organizational or in-house counsel regarding laws applicable to recording video conferences.
- Consider sensitivity of data before exposing it via screen share or uploading it during video conferences. Do not discuss information that you would not discuss over regular telephone lines.

Update to Latest Versions of Applications

Outdated or unpatched video conference applications can expose security flaws for hackers to exploit, that could result in a disruption of meeting privacy and potential loss of information, according to CISA. The agency recommends these tips to keep applications updated and secure:

- Enable automatic updates to keep software up to date.
- Develop and follow a patch management policy across the organization that requires frequent and continual application patching.
- Use patch management software to handle and track patching for your organization.
- In addition, CISA recommends organizations become familiar with security settings and capabilities of their preferred video conferencing platform(s). Here's a list of several popular products:

  Zoom
  Microsoft Teams
  GoToWebinar
  GoToMeeting
  Cisco WebEx
  Adobe Connect
  Slack

To view the article follow this link: ALTA - Tips for Secure Video Conferencing

- *Stewart's Fall/Winter Education Series – Sign up for a Webinar*

  ➢ Claims Chronicles on **December 9, 2020 at 10 AM**

  Register: HERE

If you missed our recent webinar **"Not so Basic – Policy Basics"** or are interested in other webinars we've hosted this year, check out our local Massachusetts Stewart site to view the recordings. (Scroll to the bottom to view all Webinar Recordings.)
https://www.stewart.com/content/stewart/stewartcom/en/stg/massachusetts/underwriting-resources/forms-policy-information/covid-19-info-resources.html

- *Stewart's Massachusetts COVID-19 Resource Page*

Please view our resource page which contains all the local information relative to underwriting guidance, affidavits, registry closures and frequently asked questions. This site will be updated regularly. To access click **HERE** and make it a favorite on your web-browser. You can also copy the following URL and paste it into your web browser: https://www.stewart.com/content/stewart/stewartcom/en/stg/massachusetts/underwriting-resources/forms-policy-information/covid-19-info-resources.html

200 5th Avenue, Suite 301, Waltham, MA 02451
Phone: 800-628-2988 **Fax:** 781-697-3336

Monarch Place - 1414 Main Street, Suite 1835, Springfield, MA 01144
Phone: 413-930-8090 **Fax:** 978-964-0565

Tiziano Doto, Agency Services Manager - tiziano.doto@stewart.com
Jutta R. Deeney, VP, State Counsel - jutta.deeney@stewart.com
Shannon Coleman, Underwriting Counsel - scoleman@stewart.com
Christine Provost, Associate Senior Underwriting Counsel - christine.provost@stewart.com
Tracie Kester, Underwriting Counsel - tracie.kester@stewart.com
Paula M. Cuculo, Underwriting Counsel - paula.cucoulo@stewart.com
General MA Underwriting Mailbox - massuwing@stewart.com
Tracy Hawkins, Agency Sales Representative Sr. **-** tracy.hawkins@stewart.com
Rita Kelly-Parsley, Agency Sales Representative Sr. - rita.kelly-parsley@stewart.com
Tom Potito, Agency Sales Representative Sr. **-** tom.potito@stewart.com
Mary Blomerth, Agency Sales Representative Sr. **-** mary.blomerth@stewart.com
Lyslie A. DeMeo, Agency Sales Representative, Sr. - ldemeo@stewart.com