Date of Hearing: April 11, 2023

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION Jesse Gabriel, Chair AB 1394 (Wicks) – As Amended April 10, 2023

SUBJECT: Commercial sexual exploitation: civil actions

SYNOPSIS

Child sexual abuse material, commonly referred to under the acronym "CSAM," is tragically pervasive on the internet—and not only in its illicit corners, on the so-called "dark web," but also on popular social media websites and applications that billions of people use each day. This tragedy is compounded by the fact that certain websites and applications are not only a convenient means for sharing CSAM, but arguably induce its production.

This measure proposes to address these challenges in two ways. First, the bill would require social media platforms to provide a mechanism for users to report CSAM in which they are depicted; platforms would then generally have 30 days to verify that the material is CSAM and block it from reappearing. Second, the bill would provide victims of commercial sexual exploitation the right to sue social media platforms for deploying features that were a substantial factor in causing their exploitation.

Recent author's amendments have significantly clarified the bill's functioning and are responsive to many of the concerns that have been raised by the bill's opponents.

The bill is co-sponsored by the American Association of University Women, Children's Advocacy Institute at the University of San Diego School of Law, and Common Sense Media; it is supported by six other nonprofit organizations. The bill is opposed by Electronic Frontier Foundation and an opposition coalition consisting of the California Chamber of Commerce, the Civil Justice Association of California, NetChoice, and Technet.

If passed by this Committee, this bill will next be heard by the Assembly Judiciary Committee.

SUMMARY: Requires social media platforms to provide a mechanism for users to report child sexual abuse material in which they are depicted; provides platforms 30-60 days after receiving a report to verify the content of the material and block it from reappearing. Also provides victims of commercial sexual exploitation the right to sue social media platforms for having deployed features that were a substantial factor in causing their exploitation. Specifically, **this bill**:

- 1) Defines the following terms:
 - a) "Child sexual abuse material" means either of the following:
 - i) Child pornography, as defined under federal law.
 - ii) Obscene matter, as defined under state law, that depicts a minor personally engaging in, or personally simulating, sexual conduct.
 - b) "Social media platform" and "social media company" have the same meanings as under the Business and Professions Code, except that, for purposes of this bill, the term "social

media platform" is deemed to exclude standalone direct messaging services that provide end-to-end encrypted communication.

- c) "Reporting user" means a natural person who reports material to a social media platform using the means specified in 2) below.
- 2) Requires a social media platform to provide, in a form that is reasonably accessible, a means for a user who is a California resident to report material to the platform that the user reasonably believes meets all of the following criteria:
 - a) It is child sexual abuse material.
 - b) The user themselves is an identifiable minor depicted in the reported material.
 - c) The reported material is displayed, stored, or hosted on the social media platform.
- 3) Requires the social media platform to block material reported under 2) if the reported material meets both of the following criteria:
 - a) The reported material is child sexual abuse material.
 - b) The reported material is displayed, stored, or hosted on the social media platform.
- 4) Requires a social media platform to collect from the reporting user information reasonably sufficient to enable the platform to contact the user in writing. The contact method, such as a mailing address, a telephone number (to send text messages), or an email address, must be chosen by the reporting user, and not be within the control of the social media company that owns or operates the social media platform.
- 5) Requires the social media platform to meet the following schedule of written communications with the reporting user, using the contact method collected under 4):
 - a) Within 24 hours, the reporting user must be notified that the platform received their report.
 - b) Every seven days thereafter, the reporting user must be provided an update as to the status of the social media platform's handling of the reported material, until a final written determination is issued under c).
 - c) No later than 30 days after the material was first reported, the platform must issue a final written determination stating one of the following:
 - i) The reported material has been determined to be child sexual abuse material that was displayed, stored, or hosted on the social media platform and has been blocked on the social media platform.
 - ii) The reported material has been determined not to be child sexual abuse material.
 - iii) The reported material has been determined not to be displayed, stored, or hosted on the social media platform.

- 6) Provides that if the social media platform cannot comply with the requirements in the timeframe set forth above, due to circumstances beyond its reasonable control, then:
 - a) The platform must comply with these requirements no later than 60 days after the date on which the material was first reported.
 - b) The platform must provide written notice of the delay to the reporting user no later than 48 hours from the time the social media platform knew the delay was likely to occur, using the contact method collected under 4).
- 7) Holds a social media company liable to a reporting user if it fails to comply with the requirements in paragraphs 2) 6. Available remedies include:
 - a) Any actual damages sustained by the reporting user as a result of the violation.
 - b) Statutory damages of no more than two hundred fifty thousand dollars (\$250,000) per violation. In determining the amount of statutory damages, the court is to consider the willfulness and severity of the violation, as well as previous violations by the social media company.
 - c) Costs of the action, together with reasonable attorney's fees, as determined by the court.
 - d) Any other relief that the court deems proper.
- 8) Establishes a rebuttable presumption that a social media platform that fails to comply with the requirements in paragraphs 2) 6) within 60 days of the date on which child sexual abuse material was first reported is liable to the reporting user for statutory damages.
- 9) Declares that nothing in this bill limits or impairs in any way a cause of action for deceit involving an intentional misrepresentation of fact.
- 10) Makes uncodified findings and declarations in support of the foregoing provisions.
- 11) Holds social media platforms liable if they knowingly, recklessly, or negligently facilitate, aid, or abet commercial sexual exploitation of minors.
- 12) Defines "facilitate, aid, or abet" as the deployment of a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation.
- 13) Provides that a court is to award statutory damages of between \$1,000,000 and \$5,000,000 for each act of commercial sexual exploitation facilitated, aided, or abetted by the social media platform.
- 14) Provides that the requirements of this bill cannot be waived.
- 15) Includes a severability clause that governs the provisions of this bill.
- 16) Makes technical and clarifying amendments to existing statutes.

EXISTING FEDERAL LAW:

- 1) Establishes, under Section 230 of the Communications Decency Act, that no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. (47 U.S.C. § 230(c)(1).)
- 2) Exempts from Section 230 protection violations of federal criminal law; intellectual property law; state law that is consistent with Section 230; communications privacy law; and sex trafficking law. (47 U.S.C. § 230(e).)
- 3) Defines "child pornography" as any visual depiction of sexually explicit conduct, where any of the following is true:
 - a) The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.
 - b) The visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.
 - c) The visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. (18 U.S.C. § 2256.)

EXISTING STATE LAW:

- 1) Defines "social media platform" as a public or semipublic internet-based service or application that has users in California and that meets both of the following criteria:
 - a) A substantial function of the service or application is to connect users in order to allow them to interact socially with each other within the service or application. (A service or application that provides email or direct messaging services does not meet this criterion based solely on that function.)
 - b) The service or application allows users to do all of the following:
 - i) Construct a public or semipublic profile for purposes of signing into and using the service or application.
 - ii) Populate a list of other users with whom an individual shares a social connection within the system.
 - iii) Create or post content viewable by other users, including, but not limited to, on message boards, in chat rooms, or through a landing page or main feed that presents the user with content generated by other users. (Bus. & Prof. Code § 22675(e).)
- 2) Defines "social media company" as a person or entity that owns or operates one or more social media platforms. (Bus. & Prof. Code § 22675(d).)
- 3) Defines "obscene matter" as matter, taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently offensive way, and that, taken as a whole, lacks serious literary, artistic, political, or scientific value. (Pen. Code § 311.)

- Defines the tort of deceit as including an intentional misrepresentation of fact, i.e., the suggestion, as a fact, of that which is not true, by one who does not believe it to be true. (Civ. Code § 1710(1).)
- 5) Defines "commercial sexual exploitation" as an act committed for the purpose of obtaining property, money, or anything else of value, in exchange for, or as a result of, a sexual act of a minor or a nonminor dependent. The definition includes, but is not limited to, the crimes of (i) sex trafficking of a minor, (ii) pimping of a minor, (iii) pandering of a minor, (iv) procurement of a child under 16 years of age for lewd and lascivious acts, (v) solicitation of a child for an act of prostitution, and (vi) sexual exploitation of a minor. (Civ. Code § 3345.1.)

FISCAL EFFECT: As currently in print this bill is keyed non-fiscal.

COMMENTS:

1) **Background.** Child sexual abuse material, commonly referred to under the acronym "CSAM," is tragically pervasive on the internet—and not only in its illicit corners, on the so-called "dark web," but also on popular social media websites and applications that billions of people use every day. In 2020, household names such as Discord, Reddit, TikTok, Twitch, and Twitter each self-reported thousands of instances of CSAM on their systems to the National Center for Missing & Exploited Children; Facebook reported millions. (NCMEC, 2020 *CyberTipline Reports by Electronic Service Providers* (2021), *available at* https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf.)

This tragedy is compounded by the fact that certain websites and applications are not only a convenient means for sharing CSAM, but arguably induce its production:

A Forbes review of hundreds of recent TikTok livestreams reveals how viewers regularly use the comments to urge young girls to perform acts that appear to toe the line of child pornography—rewarding those who oblige with TikTok gifts, which can be redeemed for money, or off-platform payments to Venmo, PayPal or Cash App accounts that users list in their TikTok profiles. (Levine, *How TikTok Live Became 'A Strip Club Filled With 15-Year-Olds,* ' Forbes (Apr. 27, 2022)

This measure proposes to address these challenges in two ways. First, the bill would require social media platforms to provide a mechanism for users to report CSAM in which they are depicted; platforms would then generally have 30 days to verify that the material is CSAM and block it from reappearing. Second, the bill would provide victims of commercial sexual exploitation the right to sue social media platforms for deploying features that were a substantial factor in causing their exploitation.

Recent author's amendments have significantly clarified the bill's functioning and are responsive to many of the concerns that have been raised by the bill's opponents.

2) Author's statement. According to the author:

We are not serious about ending the horror of sexual exploitation and trafficking of children if we do not aggressively address the prominent role gigantic social media platforms knowingly play in facilitating such exploitation and trafficking and re-traumatizing survivors for a lifetime afterwards.

Social media platforms that simply avoid being directly involved or active participants in child sexual exploitation in the first place and who respond with a minimum of compassion to the pleas of survivors to remove images and videos documenting their abuse have nothing to fear from this measure.

3) This bill is meant to ensure that social media platforms promptly block child sexual abuse material reported by victims. This bill establishes a comprehensive process for users to report material that they reasonably believe to be (i) CSAM, (ii) in which the users themselves are depicted as identifiable minors, and (iii) displayed, stored, or hosted on a social media platform. Following a report, a platform would have 30 days (with a potential extension to 60 days, if required by factors beyond the platform's control) to verify whether the material is CSAM, and if it is, block it from appearing on the platform. The steps in this process are set forth in paragraphs 2) - 6) of the **SUMMARY** above. Some important points to note about this process are as follows.

• Social media platforms can use a third-party service to collect CSAM reports, and thereby avoid incurring liability that might arise from coming into possession of CSAM, particularly CSAM that is not already present on their systems.

Federal law already requires online electronic service providers in the United States to report to the CyberTipline operated by the National Center for Missing & Exploited Children (NCMEC), a federally-chartered nonprofit, if they become aware of apparent CSAM that is within their control. (18 U.S.C. § 2258A.)

This bill does not specify that social media platforms must rely on NCMEC; they are free, to the extent permissible under federal and state law, to use another method of reporting. And if social media companies protest that NCMEC lacks the resources to handle an anticipated influx of reports under this bill, they can fund NCMEC directly rather than forcing the organization to rely on federal funding, currently at \$40 million per year.

The key difference between this bill and the federal law cited above is that, under this bill, social media platforms would be required to block reported material from re-appearing once it is verified to be CSAM. There is currently no such requirement under federal law.

• Social media platforms would only be required to block the specific CSAM reported by users.

Opponents of this bill protested that, under the original version of this bill, "To avoid liability, companies must be perfect and catch every attempted upload of the material, even altered versions or reproductions, which is impossible to achieve." As amended, the bill would only require that social media platforms block the CSAM that a user reports, not alterations or variations. NCMEC's Take It Down tool, funded by Meta (Facebook's parent), "works by assigning a unique digital fingerprint, called a hash value, to nude, partially nude, or sexually explicit images or videos of people under the age of 18. Online platforms can use hash values to detect these images or videos on their services and remove this content." (NCMEC, *Take It Down*, available at https://takeitdown.ncmec.org/.) Once a hash is generated, social media platforms can use it to not only remove existing copies of the CSAM, but also rapidly compare

image and video files that users attempt to upload for a match, analogous to the process that they use to scan incoming files for computer viruses.

• Social media platforms must acknowledge user reports and keep reporting users updated on the progress of their requests.

A complaint among some users who report CSAM to social media platforms is that they have no idea whether the platform has acted, or will act, to block the offending material. In such cases, survivors may "feel they have been left with no option but to take it upon themselves to monitor the presence of their own child sexual abuse images while attempting to get companies to remove it from their platforms." (Canadian Centre for Child Protection, *Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms* (2020) p. 7, *available at* https://protectchildren.ca/pdfs/C3P_ReviewingCSAMMaterialReporting_en.pdf.)

In response, this bill requires platforms to provide written updates to reporting users (i) when they submit reports, (ii) every seven days thereafter, and (iii) upon resolution of their report. Any delays beyond the statutorily-mandated 30 days must also be promptly reported to users. Finally, users must be able to choose the method by which they will receive these written updates.

• Social media platforms would retain the ability to pursue users who make fraudulent reports.

One criticism that bill opponents made of the original bill is that "if a bad actor wants to silence another user, they will report their account or content as CSAM or exploitation material." This is a well-known phenomenon. A recent ProPublica story described scammers who attempt to get influencers banned on social media platforms, on behalf of rival influencers, for a fee. (Silverman and Fortis, *A Scammer Who Tricks Instagram Into Banning Influencers Has Never Been Identified. We May Have Found Him*, ProPublica (Mar. 26, 2023), *available at* https://www.propublica.org/article/instagram-fraudster-ban-influencer-accounts.)

In response, this bill has been amended to make clear that its provisions "shall not be construed to limit or impair in any way a cause of action under [Civil Code section 1710 (1)]," i.e., for an intentional misrepresentation of fact. If a fraudster uses the mechanism specified by this bill to report an influencer or creator's non-CSAM image or video as CSAM in an attempt to get a social media platform to block it, nothing in this bill would protect that fraudster from civil liability for fraud damages. Both the person who created the content and the platform itself would have standing to sue for fraud in such a case.

Further, the requirement that social media platforms collect users' contact information in order to provide them with written updates on the status of their reports could assist platforms, influencers, and creators in pursuing users who falsely report that images or videos are CSAM in an attempt to have this content blocked.

• Standalone services that provide end-to-end encryption for direct messages are exempted from the bill's requirements.

Bill opponents protest that they "do not moderate or monitor direct messages between users because those messages are intended to be private between consumers." As amended, this bill would not apply to standalone applications that provide 100% end-to-end encrypted direct messaging, as such services play an important role in ensuring the privacy of sensitive

communications, such as political organizing and obtaining information about reproductive healthcare. But the bill would expect platforms to scan content shared through unencrypted messaging services, or through encrypted services integrated with other social media features, to block reported CSAM—just as these platforms scan uploaded material for computer viruses.

In conclusion, given the factors discussed above, it appears that the bill, in its present form, provides a targeted method for victims to report material that they reasonably believe to be CSAM in which they are depicted, and for social media companies to block this material from reappearing on their platforms, if it is verified to be CSAM. Both social media companies and injured third parties would retain the ability to sue users who make fraudulent reports of CSAM.

4) What this bill would do & analysis: holding platforms liable if they cause commercial sexual exploitation. Existing California law holds adults civilly liable for the tort of commercial sexual exploitation: sexually exploiting minors in exchange for money, property, or something else of value. This bill proposes to extend such liability to social media platforms that knowingly, recklessly, or negligently facilitate, aid, or abet commercial sexual exploitation.

As originally introduced, this provision drew significant opposition due to its definition of "facilitate, aid, or abet" as "includ[ing], but...not limited to, being directly involved in, or actively participating in, the development, deployment, or enforcement of a system, design, feature, or affordance that the social media platform knows, or should know, foreseeably causes child users to be victims of commercial sexual exploitation."

Opponents protested:

- "This provision is vague, doesn't give platforms clear direction, runs afoul of established [F]irst [A]mendment principles and is preempted by federal law."
- "Any forum or message board where users can interact with each other could be used by a predator to connect with potential victims. All those features are central to the primary functions of a social media platform and would have to be disabled to avoid liability."
- "This bill creates liability for platforms based on third party content by applying to any feature that allows users to encounter content. It effectively assumes all features are harmful and imposes liability on a site for offering any of those potentially harmful features. Platforms' algorithms and features that allow users to encounter or share content from other users are inextricably linked to the underlying content."

In response, this bill has been amended to meaningfully clarify the standard by which social media platforms could be held liable for commercial sexual exploitation. "Facilitate, aid, or abet" is now defined as "deploy[ing] a system, design, feature, or affordance that is a substantial factor in causing minor users to be victims of commercial sexual exploitation." The "substantial factor" test is generally understood to be the appropriate causation standard under California tort law. (*Rutherford v. Owens-Illinois, Inc.* (1997) 16 Cal. 4th 953, 968-9.)

It is critical to note that the bill focuses on the system, design, feature, or affordance at issue, not particular content accessible through the site. This wording is meant to insulate the provision in question from being struck down under Section 230 of the federal Communications Decency Act, 47 U.S.C. § 230(c). "The touchstone of section 230(c) is that providers of interactive computer services are immune from liability for content created by third parties." (*Fair Housing*

Council of San Fernando Valley v. Roommates.com, LLC (9th Cir. 2007) 489 F.3d 921, 925, *aff'd en banc* (9th Cir. 2008) 521 F.3d 1157.) There are limits to Section 230's preemptive effects, however; the law is "not meant to create a lawless no-man's-land on the Internet." (*Ibid.*, 521 F.3d at 1164.)

Lemmon v. Snap (9th Cir. 2021) 995 F.3d 1085, 1094 provides that even under Section 230, interactive computer services "face the prospect of liability, even for their 'neutral tools,' so long as plaintiffs' claims do not blame them for the content that third parties generate with those tools." In *Lemmon*, the Ninth Circuit held that Section 230 did not immunize social media provider Snap, Inc. for a personal injury suit brought by the parents of teen-agers who died in a high-speed traffic accident while driving 113 miles per hour. As described by the court:

Shortly before the crash, Landen [one of the teens] opened Snapchat, a smartphone application, to document how fast the boys were going. To keep its users engaged, Snapchat rewards them with "trophies, streaks, and social recognitions" based on the snaps they send. Snapchat, however, does not tell its users how to earn these various achievements. The app also permits its users to superimpose a "filter" over the photos or videos that they capture through Snapchat at the moment they take that photo or video. Landen used one of these filters—the "Speed Filter"—minutes before the fatal accident on May 28, 2017. [...]

Many of Snapchat's users suspect, if not actually "believe," that Snapchat will reward them for "recording a 100-MPH or faster [s]nap" using the Speed Filter. [...]

Snapchat allegedly knew or should have known, before May 28, 2017, that its users believed that such a reward system existed and that the Speed Filter was therefore incentivizing young drivers to drive at dangerous speeds. Indeed, the Parents allege that there had been: a series of news articles about this phenomenon; an online petition that "called on Snapchat to address its role in encouraging dangerous speeding"; at least three accidents linked to Snapchat users' pursuit of high-speed snaps; and at least one other lawsuit against Snap based on these practices. While Snapchat warned its users against using the Speed Filter while driving, these warnings allegedly proved ineffective. And, despite all this, "Snap did not remove or restrict access to Snapchat while traveling at dangerous speeds or otherwise properly address the danger it created." (*Ibid.* at 1088-90.)

The Ninth Circuit concluded that "because the Parents' claim neither treats Snap as a 'publisher or speaker' nor relies on 'information provided by another information content provider,' Snap does not enjoy immunity from this suit under 230(c)(1)." (*Ibid.* at 1087.)

The liability standard under this bill would not be easy to meet. Because of Section 230, the ability to share digital images or videos on a social media platform, in and of itself, is likely to be insufficient to trigger liability—even if the images or videos shared were produced as a result of commercial sexual exploitation. Moreover, the Ninth Circuit did not rule on whether the *Lemmon* plaintiffs had adequately pled (much less proven) that Snapchat had legally caused the accident in question by releasing the Speed Filter. But, as now worded, it appears that the bill would allow social media platforms to be held liable for deploying features that cause commercial sexual exploitation without running afoul of Section 230. To the extent this dissuades platforms from deploying features that induce commercial sexual exploitation, in much the way that the Snapchat Speed Filter allegedly induced dangerous speeding, this appears a beneficial measure.

5) **Related legislation.** AB 1282 (Lowenthal, 2023) would require the state Mental Health Services Oversight and Accountability Commission to report to the Legislature a statewide strategy to understand, communicate, and mitigate mental health risks associated with the use of social media by children and youth. The bill is currently referred to the Assembly Health Committee.

SB 287 (Skinner, 2023) would prohibit a social media platform from using a design, algorithm, practice, affordance, or feature that the platform knows or should have known causes child users to experience specified harms, including receiving content that facilitates purchase of a controlled substance and developing an eating disorder. The bill is currently referred to the Senate Judiciary Committee.

AB 2273 (Wicks, Chap. 320, Stats. 2022) established the California Age-Appropriate Design Code.

AB 2408 (Cunningham, 2022) would have prohibited a social media platform from using a design, feature, or affordance that the platform knows, or should know by the exercise of reasonable care, causes a child user to become addicted to the platform. The bill was held in the Senate Appropriations Committee.

AB 1138 (Gallagher, 2019) would have prohibited a for-profit social media website or application from allowing a person under 16 years of age to create an account without first obtaining the consent of the person's parent or guardian. The bill was vetoed by Governor Newsom.

AB 2105 (Maienschein, Chap. 166, Stats. 2018) authorized treble damages in a civil action brought by, or on behalf of, or for the benefit of, a person who is a minor or nonminor dependent and is a victim of commercial sexual exploitation.

ARGUMENTS IN SUPPORT: LookUp.Live lauds the agency this bill would provide survivors:

We...appreciate that this bill also empowers survivors haunted by the prospect of images and videos about them lingering on platforms to require this content be rendered invisible, with the ability to recover penalties against platforms that deny their requests.

Bill sponsor Children's Advocacy Institute at the University of San Diego School of Law justifies the substantial statutory damages under this bill, as follows:

[The bill] aims to offer survivors a pathway to obtaining the money needed to pay for their ongoing treatment and their suffering. It is also a harm prevention measure that seeks to impose a downside financial consequence for a platform that is directly involved in or actively participating in the sexual exploitation of children

ARGUMENTS IN OPPOSITION: An opposition coalition, consisting of the California Chamber of Commerce, the Civil Justice Association of California, NetChoice, and Technet, warns that this bill could inadvertently harm minors:

[P]latforms could choose to disable features that could be misused by perpetrators to traffic children, such as direct messaging, chat forums, or other communicative features. They could also prohibit anyone under the age of 18 from using their platforms. In either instance, more

lawful speech is impacted and burdened than intended, thus creating a chilling effect on providing and hosting lawful content and speech on social media platforms. Though well-intentioned, this bill will result in more lawful speech being removed and fewer online spaces for teens to communicate and share ideas with one another.

Electronic Frontier Foundation raises First Amendment concerns:

The design features, algorithms, and other tools social media companies use to disseminate, promote, or otherwise order content on their platforms are protected speech. Just as a newspaper must have the right to use their editorial judgment over the layout of articles in its publication, so must social media companies be able to control how information spreads across their platforms.

REGISTERED SUPPORT / OPPOSITION:

Support

American Association of University Women – California (co-sponsor) Children's Advocacy Institute (co-sponsor) Common Sense Media (co-sponsor) #HalfTheStory 3Strands Global Foundation Fairplay Junior Leagues of California State Public Affairs Committee Lookup.live Safe Social Media

Opposition

California Chamber of Commerce Civil Justice Association of California Electronic Frontier Foundation NetChoice Technet

Analysis Prepared by: Jith Meganathan / P. & C.P. / (916) 319-2200