NO. 16-10197

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
PLAINTIFF-APPELLEE,

V.

MATTHEW KEYS,
DEFENDANT-APPELLANT.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF CALIFORNIA
D.C. NO. 2:13-CR-82-KJM

ANSWERING BRIEF OF THE UNITED STATES

LESLIE R. CALDWELL
ASSISTANT ATTORNEY GENERAL

JAMES SILVER
DEPUTY CHIEF

FRANK LIN
TRIAL ATTORNEY
U.S. DEPARTMENT OF JUSTICE
CRIMINAL DIVISION
COMPUTER CRIME & INTELLECTUAL
PROPERTY SECTION

PHILLIP A. TALBERT
ACTING UNITED STATES ATTORNEY

CAMIL A. SKIPPER
ASSISTANT U.S. ATTORNEY
APPELLATE CHIEF

AUSA MATTHEW D. SEGAL
AUSA PAUL A. HEMESATH
ASSISTANT U.S. ATTORNEYS
EASTERN DISTRICT OF CALIFORNIA
501 I STREET, SUITE 10-100
SACRAMENTO, CALIFORNIA 95814
TELEPHONE: (916) 554-2700

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

STATEMENT OF JURISDICTION

The district court had jurisdiction pursuant to 18 U.S.C. § 3231. Judgment was entered on May 5, 2016, and amended for restitution on July 7, 2016. ER 190-95, 176-189. Keys filed a timely notice of appeal on April 25, 2016. Fed. R. App. P. 4(b); ER 168-69. This Court has jurisdiction pursuant to 28 U.S.C. § 1291.

ISSUES PRESENTED FOR REVIEW

1. The indictment contained a broad allegation that Keys kept and used for malicious purposes login credentials to his former employer's network. Did the government constructively amend the indictment when it offered evidence of the specific malicious ways in which Keys used those login credentials?
2. Did the district court abuse its discretion in admitting evidence that Keys sent a command to his former employer's network to obtain a customer list and then used that list to send emails to raise panic at the employer, made admissions about his hacking activity, and tried to alienate customers? Did the district court

plainly err in admitting evidence Keys sent commands to the network to create more "back door" login credentials and lock his replacement out of the network?

3. Did the district court abuse its discretion by instructing the jury in the plain language of a criminal statute?
4. Was the evidence sufficient for the jury to find that Keys attempted to cause damage to a newspaper's website when he sent unsuccessful logon commands to help a confederate post a defaced front-page layout?
5. Did the district court abuse its discretion by ordering restitution in the amount of estimated lost time of salaried employees and the value of a marketing program that Keys had ruined in the course of his crime?

BAIL STATUS

Keys is serving the sentence imposed in this case. His projected release date is April 30, 2018.

STATEMENT OF THE CASE

I. Procedural History

On March 14, 2013, the grand jury indicted Keys for conspiracy to transmit code to cause damage (count one), transmitting code to

cause damage (count two), and attempted transmission of code to cause damage (count three). ER 244-52. The charge period covered December 8-15, 2010, when Keys conspired with members of the "Anonymous" hacking group to deface the *Los Angeles Times*. On December 4, 2014, the grand jury returned a superseding indictment. ER 235-243. The superseding indictment charged the same crimes, but expanded the charge period in count two to October 28, 2010, through January 3, 2011, and added to each count the allegation that before Keys connected with Anonymous, but after his employment was terminated, Key "kept and used, for malicious purposes," login credentials to his former employer's network. 18 U.S.C. § 371, 1030(a)(5)(A), 1030(c)(4)(B), 1030(b); ER 236, count 1, ¶ 1(h); ER 239, count 2, ¶ 1; ER 240 count 3, ¶ 1.

On September 25, 2015, the district court heard motions in limine. SER 172-225. The eight-day trial began on September 28, 2015. CR 108. On October 7, the jury convicted Keys on all three counts. CR 120.

On April 13, 2016, the court sentenced Keys to twenty-four months imprisonment. ER 170-01. On June 8, 2016, the court heard

argument on restitution and ordered Keys to pay $249,956.00. SER 1-16; CR 168.

II. Factual Overview

Keys was the web producer and a computer network site administrator for KTXL FOX40, a Tribune Company television station in Sacramento. PSR ¶ 6. On October 28, 2010, Keys became an angry former employee. PSR ¶ 5. When he left the company, he had some computer skills and a set of passwords that had tremendous powers on the network that Tribune Company used to publish web content for all of its print and broadcast outlets. PSR ¶ 6. Log files for that system show that Keys was active on it hundreds, if not thousands, of times after he was sent home from work. SER 694.

Keys used this access for a two-month-long campaign of payback that had five components: (1) he obtained a customer list from the network and used it to send pseudonymous emails in which he taunted that he had access to the network and it was not secure; (2) he locked his newsroom replacement out of the network; (3) he created more back-door login credentials; (4) he passed those login

credentials to a group of hackers and helped them deface a story on the home page of the *Los Angeles Times*; and (5) after the defaced story was removed, Keys worked with the story defacer to try to post an entire defaced front page on the newspaper's web site. PSR ¶¶ 6-12.

The superseding indictment charged three crimes. Count one charged conspiracy to cause damage to a protected computer. 18 U.S.C. § 371. Count one was based on Keys's conspiracy with other hackers and covered the period during which they worked together to deface the *Los Angeles Times*. Count two charged a substantive count of transmission of malicious code causing loss over a time period less than one year. 18 U.S.C. § 1030(a)(5)(a), (c)(4)(B). Count two was based on the malicious conduct that Keys carried out on the network by himself before conspiracy and with confederates during the conspiracy. Count three charged attempted transmission of malicious code based on Keys's and a confederate's attempt to post a defaced front page on a Tribune Company newspaper. 18 U.S.C. § 1030(a)(5)(a), (b).

III. Keys used backdoor network credentials and the help of others to engage in a campaign of payback against his former employer.

A. Keys's boss sent him home, tried to lock him out of the network, and hurt his feelings.

Matthew Keys was the web news producer for FOX40. FOX40 was part of the Tribune Company family of television, radio, and print media outlets. SER 578-80. All of Tribune Company's twenty-three broadcast stations and fourteen newspapers used the same content management system ("CMS") to publish their news and other content to the Internet. SER 578-80. Keys was also a site administrator for the Tribune CMS. SER 524. It was part of his job to train new employees on the system, post content to the system, and assist others with their passwords and log-in issues. SER 523-24.

Friday, October 28, 2010, was Keys's last day as an employee at FOX40. SER 237. Brandon Mercer, FOX40's News Director, sent Keys home after the two had a loud disagreement in the news room. SER 236, 525. Mercer wanted to lock Keys out of the CMS, so he ordered Tribune Company's information technology department to change the password to Keys's CMS user account "mkeys." SER 237.

On Monday, Mercer returned to the office to find that Keys's personal belongings were gone. SER 239. Keys felt hurt and wanted there to be consequences. SER 828, 830 (audio).

B. Keys still exercised network powers using back door accounts and a foreign IP address.

Even after his boss sent him home and changed his CMS user account password, Keys remained well equipped to make hard-to-attribute trouble for his former employer. Keys still had other username/password combinations and, moreover, the ability to create entirely new user accounts. SER 820 (audio), 851. Keys had also discovered that he could use a virtual private network ("VPN") service called "Overplay" to mask his true IP address. SER 826, 828 (audio); 642-45. Overplay provided an Internet service analogous to call forwarding, which allowed its users to appear to be connecting to the Internet from IP addresses outside the United States. SER 642-45.

C. Keys used Tribune Company CMS credentials for a malicious email campaign.

Keys began his payback campaign within days of clearing out his desk. First, on November 3 and November 22, Keys, through the

Overplay VPN, used a "super user" account test1234 to send a "GET" command and order the CMS to download to him a list of FOX40 viewer email addresses. SER 476, 481-82, 806, 842-44. Tribune Company had collected these emails from participants in the FOX40 Rewards program, which had been designed to promote ratings. SER 230. Rewards viewers gave FOX40 their emails, phone numbers, and addresses. SER 231. Some also put in credit card information. SER 330. Keys obtained the list again in December. SER 806.

Keys used the email list for what he later told the FBI was "hooliganism." SER 925 (audio). On December 1, 2010, Keys sent his former manager, the FOX40 News Director, a series of pseudonymous emails from different email addresses named after characters from "The X-Files" television show. *See, e.g.*, SER 250-51, 770. These emails purported to come from a group that had breached the CMS and obtained a list of FOX40 Rewards email addresses. *See, e.g.*, SER 770-74, 784. The emails taunted that Tribune Company's network was not secure and that entities such as FOX40 could not protect their systems from determined insiders who "go rogue." SER 786, 796. When Mercer warned the "group" about

the legal consequences of sending out emails to the stolen list, Keys responded that identifying the source of the breach would require "a long and painstaking process," likely to be complicated by "the laws of the countries where we reside and whether or not they're up to playing ball with the federal investigators in your country." SER 775-76.

Mercer that same day contacted Tribune Company in Chicago. The Tribune Company employees who ran the CMS pulled over 5,000 pages of server logs to identify what FOX40 user accounts would have had access to viewer information. *See* SER 253, 589, 795. They reset passwords for some FOX40 employees' CMS accounts and deleted others. *See* SER 253, 589, 795.

The next day, Keys used the FOX40 Rewards list and his pseudonymous accounts to send emails to viewers. SER 781. The emails were critical of the station and asked viewers whether FOX40 was "spying on you, turning your credit card statement into advertising GOLD." SER 783. As a result, viewers called the station worried about the security of their bank accounts and credit cards. SER 331-32. FOX40 staff spoke with complaining customers both to

reassure them and try to learn about the underlying breach. SER 331-32. The emails to viewers continued through at least December 6. SER 786-88. Keys later told the FBI that he thought that his email campaign "terrified" his former boss. SER 831 (audio).

D. Keys used his CMS credentials to lock his newsroom replacement out of the CMS.

Keys also repeatedly reset the CMS account password used by his replacement Samantha Cohen. This did to Cohen what Mercer had tried to do to Keys: it locked her out of the CMS.

When Keys left FOX40, his responsibilities were reassigned to Cohen. SER 268, 526. On December 6, the day of the last recorded communication to viewers in the email campaign, Cohen began experiencing extraordinary problems logging into the CMS.[1] SER 787-88, 269-70. Cohen was in constant communication with support personnel to resolve her logon problems. SER 789-94. Cohen

[1] Cohen was also supposed to start managing FOX40's Facebook and Twitter accounts but she could not log into those accounts either. SER 527-28. FOX40 worked directly with Twitter and Facebook to gain control of its accounts. SER 240-41, 306-07. In the meantime, thousands of FOX40's Twitter followers had been deleted. SER 239, 466.

testified that, as a result of her inability to access the CMS, she could not work for five days. SER 546-47, 573-75; 789-94. According to Tribune Company and Overplay server logs, Cohen was unable to access her CMS account because Keys had been using the foreign VPN to anonymously log onto the CMS and repeatedly change Cohen's credentials. SER 675-76.

E. Keys created back doors on the CMS.

Keys also created "back door" CMS credentials. According to trial testimony:

> In security terms, a back door is a way for an attacker or a hacker to regain access. And so generally if the original way they were able to break into the system, if that is terminated or if that access is no longer available, an attacker will try to establish a back door, which is a way that they can gain access again. And so in the house analogy, you know, a back door would be as simple as maybe someone, you know, unlocking a window on the side of the house.

SER 466. On December 8, Keys edited a user group to create a backdoor in the form of an unassigned user account, "anon1234." SER 473-74; 644-48.

F. The *Los Angeles Times* Defacement.

On December 12, 2010, Keys, using his true name, emailed FOX40's News Director and advised that he had a scoop: Keys had infiltrated the hacker activist collective Anonymous. SER 787-801. In email and over the phone, Keys told Mercer that he had access to future Anonymous operations against PayPal, Amazon, and an expected attack against the *Los Angeles Times*. SER 787-801, 801 (audio), 807-812.

Keys was able to predict the attack on the *Los Angeles Times* because Keys had been instigating and facilitating such an attack. In early December, using the moniker "AESCracked," Keys entered multiple chatrooms, also known as Internet Relay Chat rooms ("IRC"), to recruit the hackers of Anonymous to attack his former employer. *See generally*, SER 807-12.

On December 8, he wrote "if you want to attack fox news, pm[2] me. i have a user/password for their cms." SER 807-12. Keys sent CMS super user credentials to Anonymous, specifically, the

[2] "PM" is a common abbreviation for private message.

anon1234 username and password, and urged the group to "go fuck some shit up!" SER 809, 811. Keys followed up by telling the group how to navigate the CMS, what Tribune Company media outlets to target, and how to create still more super user credentials that would blend in better. SER 807-12.

Keys viewed Anonymous as highly skilled hackers who could do "significant damage and not get[] caught," and had "blatant disregard for . . . any kind of law." SER 818 (audio). The "super user" account Keys had given them had "enormous power in the system" and was the kind reserved for a handful of central corporate employees. SER 474, 603-05. A super user account could be used to delete all the content on a site. SER 390. A CMS super user account could also be used to create users, delete users, and edit content in all markets. SER 389. A super user could rebrand the site, change the page layout, or create or modify archived stories deep within the site. SER 390.

Keys was clear for days about his purpose. He quickly reminded his confederates, "i did not give you those passwords for 'research.' i want you to fuck shit up." SER 863. A day later, on

December 9, Keys referred them to a particular *Los Angeles Times* article critical of WikiLeaks and wrote, "Yet another reason the Times must be demolished." SER 867. On December 10, when someone else in the chat room resisted the suggestion to attack the news media, Keys responded "FOX News is not media. it's 'infotainment' for inbreds. I say we target them." SER 868. On December 14, he again wrote, "Anyone interested in defacing FOX, LA Times? I have users/pass into their CMS." SER 869.

Despite what Keys thought of them, no one from Anonymous used the back-door super user credentials to delete an entire newspaper site from the Internet. Instead, a hacker known as "Sharpie" changed the headline, lede, and byline of a story about Congress on the *Los Angeles Times* website. SER 854, 855.

A *Los Angeles Times* editor found the defaced story on the home page while spot checking the paper's web site. SER 403-05. He regarded this as the most serious content-related security incident in his thirty-three years at the paper. SER 413. The newspaper's actual story was unavailable to readers on the desktop version of the website for forty minutes and the mobile version of the site for a day.

SER 377-81. It was not possible to just "hit a button" and revert the mobile site to its original state. SER 380.

The result at Tribune Company headquarters in Chicago was "panic," the personal involvement of the Chief Technology Officer, and a report to the Chief Executive Officer. SER 596-97. The *Los Angeles Times* had lost editorial control of its publication. According to the CMS system architect at the time, "The functionality of the *L.A. Times* website was to have news for the consumers to read and be trustworthy. The functionality of the website was to produce valid content. [The defaced story] was not valid content." SER 416. According to the *Los Angeles Times*'s online editor, the paper's loss of control of what it published threatened its core function:

> It's -- the essence of journalism is to provide useful, correct, accurate information to the public. That's what our business is built around. It's the core reason we exist. And that information needs to be reliable. If people come to our website, and they see it messed up for that or any other reason, they're going to not trust it. Trust is all we've got. That's what the business is.

SER 349. This view was shared by the *Los Angeles Times* editor who discovered the defacement: "Our reputation, the reputation of a

newspaper depends on what we publish. And we, you know, need to be in charge and aware of what's going up on our website just as much as we do -- you know, just as we did going into the print edition." SER 401.

After the *Los Angeles Times* was attacked and it was discovered that unauthorized super user accounts had been created that outsiders could use to edit the paper, Tribune Company's response became far more robust. A large team spent that night locating unauthorized super user accounts and shutting down any other such back-door access points. SER 603-05. Immediately after discovering the alteration, multiple employees in the *Los Angeles Times* editorial division and Tribune Company information technology division spent urgent hours trying to correct the story and determine how the unauthorized alterations were made. Every Tribune Company CMS user account was locked and each user was told to reset her password. SER 392-94, 436, 589. To re-secure the system, they identified and deleted any user account not associated with a then-current employee. SER 615-18. This resulted in journalists in

several newsrooms having trouble logging on because of all the activity required by the incident response. SER 616.

According to Tribune Company's managing director in charge of the architecture of all of Tribune's computer systems, closing all back doors was necessary to restore system integrity. "Back doors" on a news site compromise its core function to publish as news only what content the news organization directs. "Ngarcia" was the backdoor used to deface the *Los Angeles Times* story. The system architect testified as follows:

> Q. The fact that you found N. Garcia to be an unauthorized user, what effect did that have on system integrity?
>
> A. The system was designed to allow users who were authorized to generate content with editorial integrity, to put that content on the business website, which was the product of the company. If that information and product was not in line with the spirit of the company's being an editorial news agency, it would compromise the value of the company and its integrity as a news source.
>
> Q. What about the integrity of the security of the system?
>
> A. The integrity of the system would mean that we cannot ensure that anyone who had access was of -- was appropriate.

> Q. Is that why you asked everyone to change their passwords?
>
> A. Yes.

SER 455; *see also* SER 429-31, 451.

Jason Jedlinski, who was a vice president of products for the Tribune Company digital division, testified that finding and deleting unauthorized user accounts was the most important thing that Tribune Company had to do immediately to restore system integrity. SER 487-88, 617-18.

G. Keys and a co-conspirator tried to alter the entire front page of the *Los Angeles Times*.

Shortly after the attack and Tribune Company's subsequent mass-deactivation of CMS user credentials, Keys and Sharpie again corresponded via Internet chat. Sharpie told Keys that he "had a whole front page layout" to post to the CMS, but had difficulty accessing the CMS.[3] SER 856. Keys then replied that he could provide access to the CMS, writing: "I can grant you access again . . . Standby. Have to use VPN to cover my tracks . . . damn they cut off

[3] In the IRC transcript, Sharpie originally wrote that his front page layout was for the *Chicago Tribune*, but later corrected himself and clarified that the layout was for the *Los Angeles Times*.

my account . . . hang on. Nope, I'm locked out for good." SER 856-57. During this conversation, according to CMS logs, Keys was online, attempting to access the CMS. SER 691, 853, 856, 857, 686-91.

IV. Tribune's Losses

At trial, the government proved that the total dollar value of FOX40 and Tribune Company employee time spent dealing with Keys's email campaign and his mischief with his replacement's logins was between $3,605 and $4,184. SER 289-91, 546, 610-11, 711-3. At trial, the total dollar value of Tribune Company employee time spent responding to and assessing the *Los Angeles Times* defacement alone was estimated to be between $6,601 to $8,963. SER 348-60; 411-13; 390-93; 443-46; 463-64, 494; 497, 504-05; 610-22.

Tribune Company took until January 2011 to complete its damage assessment. SER 508. They did not know if the hackers had jumped off to other systems, deleted logs of their activity, and/or created accounts to gain access to financial information. SER 499. Tribune Company employees had to review thousands of pages of archives to ascertain whether the breach had affected the systems

that controlled log-in authentication, financial systems, or even the newspaper printing plates. SER 499-505.

Keys's email campaign "had the effect of engendering hostility and distrust among the viewers who had signed up for the loyalty program." PSR ¶ 7. Viewers had been told that FOX40 had allowed a database with their credit card information to be compromised. PSR ¶ 7; SER 330-32; 781-83, 997-98. Of the 20,000 people who had signed up, all but 1,000 cancelled their participation. PSR ¶ 7; SER 330-32; 781-83, 997-98. Tribune Company had to build an entirely new database of viewers. PSR ¶¶ 14-15. Further, there were other Tribune Company employees whose salaries and time were not offered at trial but who worked on the incident. SER 505-08.

V. Keys "objected" to the new allegation in the superseding indictment, but did not submit a jury instruction limiting the jury's consideration of the evidence.

The superseding indictment expanded the charge period to October 28, 2010, through January 3, 2011, and added the following broad narrative allegation: "After his employment was terminated, MATTHEW KEYS kept and used, for malicious purposes, login credentials to the Tribune Company's CMS." ER 235-43, count 1,

¶ 1(h) (re-alleged in ¶ 1 of counts 2 & 3). Although the original indictment had been limited to what Keys did in the period he was allied with Anonymous, ER 244-50, the evidence of the email campaign had been well known to Keys from the beginning. *See* CR 23 at 3-4.

The new allegation was discussed at length during the hearing on motions in limine. SER 147-48. Keys complained about the government's decision to supersede and broaden the indictment to include the email campaign. Counsel stated:

> Additionally, the Cancer Man e-mails don't really have anything to do with the trans -- they have nothing to do with the transmission of the code to the Tribune Company's servers that edited that one paragraph in the *L.A. Times* website story that are relevant. And that's why I believe the government didn't actually put them in the first indictment, but they put it in the second indictment to sort of just expand the scope and make this look a lot badder than it is.

SER 201-02. On the first day of trial, the court reminded Keys, "The indictment alleges that Keys kept and used user names and passwords for malicious purposes, including to attack FOX40." SER 161. The defense objected. SER 161. That inspired the court to ask,

"So why does it take the Court to find that language for you?" SER 161.

Keys's proposed jury instructions did not include an instruction to disregard the email campaign or resetting of the Cohen passwords. ER 165-67. Keys filed a written response to the government's instructions and did not propose limiting what evidence the jury could consider on count two. SER. 938-41.

VI. At trial, the government proved that Keys had used CMS passwords to conduct a weeks-long campaign of online retaliation against Tribune Company.

The jury heard the testimony of FOX40 newsroom employees, *Los Angeles Times* editors, and Tribune Company information technology employees. SER 227, 342, 361-62, 427-29, 495-98, 517-18, 576-78, 695-96. An FBI agent then compared CMS logs, Overplay logs, Anonymous chatroom logs, and evidence seized from Keys's own laptop to show that the email campaign, the locking out of Cohen from the CMS, the communication with Anonymous, and the final attempt to log onto the *Los Angeles Times* to post a prepared altered front page layout all pointed to Matthew Keys, who used a Macintosh computer, a Firefox web browser, Overplay, and a true IP in the

Sacramento area. SER 629-61, 647-94. The identification was corroborated by a confession that was detailed, Mirandized, audio-recorded, written out in Keys's own hand, and accompanied by his annotation of a copy of the Anonymous chatroom logs. SER 806, 807-812, 813-39, 619-20.

The CFAA element of $5,000 in loss was calculated by the monetary value of employee time. FOX40 employees testified about their salaries and their time spent responding to the email campaign. SER 289-91 (Mercer); 702-04 (Del Core). Samantha Cohen testified about the time she lost while she could not log onto the CMS. SER 546. *Los Angeles Times* editors testified about their salaries and time spent responding to the story defacement. SER 348-60 (Gaines); 411-13 (Hanrahan). Tribune Company information technology employees testified about their salaries and time spent responding to the incident and conducting damage assessment. SER 390-93 (Comings); 443-46 (Caro); 463-64, 494 (Kulesza); 497, 504-05 (Rodriguez); 610-22 (Jedlinski).

At the close of the government's case, Keys moved for a judgment of acquittal. SER 715. He argued that the evidence was

insufficient to show a substantial step towards defacing the newspaper's front page; that there had been no damage because "the CMS system operated securely" and "did everything that it was supposed to do;" that no expert testimony had been offered on the reasonableness of the cost of Tribune Company's response; and that Tribune Company's expenses associated with identifying who was sending the emails and resetting Cohen's passwords could not be loss. SER 715-16. The district court denied the motion. SER 722.

VII. The court sentenced Keys to twenty-four months of imprisonment and ordered him to pay $249,956 in restitution.

On April 13, 2016, the court sentenced Keys to twenty-four months of imprisonment on each count, to run concurrently. CR 153. For Guidelines loss purposes, the court found that trial witnesses' estimates of the value of their lost time had been proven by clear and convincing evidence (a range between $10,206 and $13,147). SER 41, 62-64. The court postponed a restitution hearing and considered as a downward variance Keys's need to work to pay restitution. SER 125-26.

Tribune Company did not submit a restitution claim. SER 22. The loss estimates were based chiefly on trial testimony about salaried employee time and an interview of Jerry Del Core, a trial witness who had been FOX40's station manager at the time of the offense, but who no longer worked for the company. PSR ¶ 14; SER 976, 850-52, 997-98, 505-08, 695-708. The PSR had calculated $249,956 based on lost employee time ($49,956) and the expense to build a new database of viewers at $10 per customer ($200,000). PSR ¶¶ 15, 80; SER 13.

The court heard argument on restitution on June 8, 2016. The chief issues were restitution for (1) employee time and (2) the effect that Keys's emails to customers had on the FOX40 Rewards program.[4] According to Del Core, the FOX40 Rewards program was run through a database called "Greenlinks." It was not just an email list, but, rather, also a way for FOX40 to accrue revenue when its

[4] Keys had issued a subpoena *duces tecum* to Tribune Media (Tribune Company's successor) for "Documents and objects relevant to the allegations of damage and loss, e.g. invoices from third parties that investigated the events alleged in the indictment, purchase orders from the LA Times and/or Tribune Media Company documenting the loss it suffered caused by the alleged damage." SER 1019. Keys produced no evidence.

viewers made online purchases. SER 997-98. "When the database was compromised people cancelled their participation . . . [I]t took three years to rebuild." SER 997-98. Del Core stated that "out of the original 20,000 accounts in the databased, only 1,000 were retained." So they started anew. SER 997-98. The value of each customer was $10. SER 997-98.

Keys first said that rounding down estimates would be acceptable and that he was "not saying zero is the right number." SER 8. A few minutes later, he argued that because the estimates of employee time were imprecise, there should be no restitution at all. SER 10. Keys objected to the $200,000 cost of building a new viewer database as "an awfully round number," (SER 12), and that even if there were "some anger issues" among participants in the FOX40 Rewards program, no restitution was appropriate because FOX40 still had its list of those customers. SER 13.

The court ordered $249,956 in restitution based on the estimates of lost time and the cost of building a new viewer database. CR 168. The court expressly referred to trial testimony of Tribune

Company employee witnesses and accepted the $200,000 estimate for the customer database. SER 13.

Tribune Company's corporate successors assigned their restitution payments to the Crime Victims Fund. CR 173.

SUMMARY OF ARGUMENT

Matthew Keys left his job angry, hurt, and able to seek payback in one way: malicious use of his continued access to Tribune Company's CMS. After he walked out of FOX40, Keys used that access to obtain the email addresses and use them to cause panic at FOX40, to lock Cohen out of her CMS account, and to create more back doors. Then Keys got others to carry out an actual and attempted defacement of the *Los Angeles Times*. There was no constructive amendment because count two of the superseding indictment covered this entire period and its broadest allegation encompassed the malicious things that Keys did with his network access after his termination.

This same conduct was admissible not only to prove the acts alleged in count two, but also as evidence of *mens rea*, motive, and identity for counts one & three (conspiracy and attempt).

Keys makes a number of objections to what the jury was allowed to "consider." He is not always clear about whether he is objecting to what the jury was allowed to hear versus how the jury was instructed. Nonetheless, the things Keys objects to were admissible and required no limiting instruction.

The court correctly denied Keys's Rule 29 motion. To find $5,000 in loss required for conviction on the substantive felony, the jury could rely on the witnesses who testified about their own work. To find an attempt, the jury's conclusion was supported by ample evidence. Keys and his co-conspirator had successfully used Keys's back-door CMS access to deface a *Los Angeles Times* article, had prepared an entire substitute front-page layout, and together attempted to log in to post it. They only failed because the CMS administrators had, in essence, changed the locks on the building since the attackers' last act of intrusion and vandalism.

Finally, the court did not abuse its discretion in calculating restitution. The amount was adequately supported by the evidence presented at sentencing, at trial, and the information of which the court took judicial notice.

Keys's specific attacks on his convictions only relate to counts two and three and to the restitution order. The sentence for count one was imposed concurrently, so this Court's resolution of Keys's appeal should not affect his period of incarceration.

ARGUMENT

I. There was no constructive amendment of count two because broad language in the superseding indictment encompassed Keys's specific conduct on the CMS prior to the *Los Angeles Times* defacement.

A. Standard of Review

This Court should review Keys's constructive amendment claim for plain error. *See United States v. Shipsey*, 190 F.3d 1081, 1085 (9th Cir. 1999). Although Keys concedes that he never explicitly raised constructive amendment before the district court, he claims that he preserved this error with a statement during the charge conference. AOB at 18 (citing *United States v. Lloyd*, 807 F.3d 1128, 1164 (9th Cir. 2015); *United States v. Ward*, 747 F.3d 1184, 1189 (9th Cir. 2014)).

Keys's statements at the charge conference did not make a timely objection. The court had ordered pretrial submission of jury instructions at a time when this issue was well known to Keys. CR

57; Fed. R. Crim. P. 30. Keys did not ask for an instruction for the jury to limit its consideration of the email campaign or the resetting of Cohen's passwords. Keys affirmatively asked for this Court's pattern instructions. ER 167-69, 938-41. At the charge conference, he merely stated, "There is a general concern, and if it arises here or somewhere else, we're not certain, that so much of the facts and information and evidence that was introduced is unrelated to what was expected out of Count Two under the superseding indictment." SER 291-92.

An objection to a jury instruction must be formal, timely, and distinctly stated. *See United States v. Klinger*, 128 F.3d 705, 710 (9th Cir. 1997). The charge conference was too late to express a vague "general concern." This Court enforces local rules like E.D. Calif. Loc. R. 163, which requires pretrial submission of jury instructions. *See United States v. Lustig*, 555 F.2d 737, 751 (9th Cir. 1977). A district court should not be reviewed de novo for disregarding the kind of "objection" Keys made. *See United States v. Sanchez-Mata*, 429 F.2d 1391, 1392 (9th Cir. 1970) ("The orally requested instruction was properly refused."); *United States v. Soto*,

519 F.3d 927, 935 (9th Cir. 2008) ("[T]he district court did not abuse its discretion by refusing to give Defendant's proposed instruction that was untimely, not in writing, not in precise form, and in violation of Rule 30(a).") (Graber, J., concurring). This case is nothing like *Ward*, in which this Court reviewed de novo a district court's decision not to give a jury instruction that had actually been proposed. *See* 747 F.3d at 1188.

B. Keys's email campaign and interference with Cohen's network access were encompassed by the broad allegation that after his job ended, Keys kept CMS login credentials and used them for malicious purposes.

Keys's constructive amendment argument to this Court relies on an incorrect statement about the superseding indictment. He claims that the superseding indictment only broadened count two's date range, "otherwise leaving the original indictment unchanged." AOB at 7. That is untrue. *Compare* ER 245, ¶ 1 with ER 236, ¶ 1(h). The superseding indictment expanded the charge period to immediately after Keys left FOX40 and added the broad allegation that, "After his employment was terminated, MATTHEW KEYS kept and used, for malicious purposes, login credentials to the Tribune

Company's CMS." ER 236 (count one, ¶ 1(h)); 239-40 (count two, ¶ 1). This allegation encompassed the specifics of the email campaign and the Cohen CMS lockouts, which all occurred after Keys left Tribune Company, involved use of CMS login credentials, and served malicious purposes.

Keys at times has understood the significance of the broad allegation. In district court, Keys complained that the "Cancerman emails" were distinct from the *Los Angeles Times* defacement and, further, "they put it in the second indictment to sort of just expand the scope and make this look a lot badder than it is." SER 202-03. Later, the court had to remind Keys of Paragraph ¶ 1(h) and asked why it took the court to find that language for the defense. SER 160. The defense only responded that they had thought about it over the weekend and objected. But the defense did not attack the superseding indictment as too vague and never moved for a bill of particulars. It is broad language, and he cannot simply wish language out of the indictment in order to manufacture a constructive amendment claim.

The government obtained a superseding indictment to include the conduct to which Keys now objects. SER 202-03. Count two charged a statutory offense that involved a loss from the defendant's weeks-long conduct. Count 2, ¶ 2 (ER 239-241). The proper inquiry for the jury was what aggregate harm Keys caused in that period, which began well before he defaced the *Los Angeles Times*. *See Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) (noting the CFAA contains "no 'single act' requirement").

If he objected to the generality of this language, Keys might have tried for a bill of particulars. But it precludes a constructive amendment claim based on specific facts that fit within the allegation. "An amendment of the indictment occurs when the charging terms of the indictment are altered, either literally or in effect, by the prosecutor or a court after the grand jury has last passed upon them." *United States v. Von Stoll*, 726 F.2d 584, 586 (9th Cir. 1984) (quotations and citations omitted).

By its nature, a constructive amendment claim has to point to something offered for conviction that cannot fit within the language of the indictment. "[W]here a generally framed indictment

encompasses the specific legal theory or evidence used at trial, no constructive amendment occurs. *United States v. Morgenstern*, 933 F.2d 1108, 1115 (2d Cir. 1991); *see also United States v. Skelly*, 442 F.3d 94, 99 (2d Cir. 2006); *United States v. Salmonese*, 352 F.3d 608, 620 (2d Cir. 2003); *United States v. Gonzales*, 436 F.3d 560, 577 (5th Cir. 2006).

Keys also knew this during the charge conference. When asked by the court, Keys essentially conceded that an acquittal in this trial would have created a double jeopardy bar against charging the defendant with the email campaign. SER 723-24.[5]

II. The district court did not abuse its discretion in admitting evidence that Keys used his post-

[5] Keys has not claimed there was a variance. He identifies no place in the record where the government misled him about how it was going to prove its case. *Compare United States v. Adamson*, 291 F.3d 606, 615-16 (9th Cir. 2002). Rather, here, there is just a broadly worded indictment that could be proven in a number of ways. *See United States v. Doss*, 630 F.3d 1181, 1191 (9th Cir. 2011) (finding no variance where indictment alleged witness tampering through identified false statements "among others" because "the indictment language in this case is more forgiving, suggesting there could be other statements beyond those alleged."). Keys was always aware of this evidence, CR 162 at 7, and within weeks of the superseding indictment, the government explicitly warned that it would be offering evidence of the email campaign to prove loss under count two. *See* SER 1034-38.

employment CMS access for various malicious purposes.

A. Standards of Review

Keys argues that the court erred in allowing the jury to "consider" various acts that he says were not CFAA "loss" or "damage." This Court "review[s] objected to evidentiary rulings for abuse of discretion, and unobjected to evidentiary issues for plain error." *United States v. Torralba-Mendia*, 784 F.3d 652, 659 (9th Cir. 2015). This Court reviews for an abuse of discretion a district court's decision that the probative value of evidence exceeds its potential for unfair prejudice. *United States v. Curtin*, 489 F.3d 935, 943 (9th Cir. 2007) (en banc). Even if this Court finds error, it will only reverse if an erroneous evidentiary ruling more likely than not affected the verdict. *See United States v. Pang*, 362 F.3d 1187, 1192 (9th Cir. 2004).

Keys objected to admission of the email campaign. Keys did not object to admission of his interference with Cohen's network credentials. When Cohen testified, the only time that Keys objected was to the question "On December 6th, do you recall having trouble with your password?" SER 529. He did not object to the other

questions. 529-565. Keys never objected to evidence that he created back doors. SER 466, 473-74, 499-504, 603-05, 638-41, 647.

B. The court did not abuse its discretion when it admitted evidence that Keys used his post-employment CMS access to carry out a malicious email campaign.

Keys asserts that copying data does not constitute damage under the CFAA. AOB at 28-30. But the evidentiary ruling he objected to at trial was the court's determination that the "Cancerman emails" were relevant. *See* AOB at 28 (citing ER 107-08). The district court did not abuse its discretion in admitting those emails.

First, the emails were relevant to the jury's finding that Tribune Company's costs amounted to at least $5,000. 18 U.S.C. § 1030(c)(4)(B). In the various emails, Keys bragged that he was part of a group that could easily access the CMS. SER 775-76, 784, 786. Tribune Company in Chicago and FOX40 in Sacramento responded immediately, trying to identify the source of the breach and stop it. SER 795, 802-04, 267, 589. This was relevant to calculate "loss," which is "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and

restoring the data, program, system, or information to its condition prior to the offense." 18 U.S.C. § 1030(e)(11). "Loss" includes costs related to the investigation of computer intrusions and any subsequent remedial measures. *See Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1074 (6th Cir. 2014) (stating loss includes costs associated with investigating the offense and conducting a damage assessment); *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 954, 963 (N.D. Cal. 2014) (acknowledging loss extends to examining what data was made unavailable and how to restore it); *Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 894-95 (N.D. Cal. 2010) (stating loss includes cost to investigate and remediate).

Second, the email campaign was probative of the *mens rea* elements of conspiracy. In the conspiracy instruction, the jury was asked whether Keys could reasonably foresee that the conspiracy would cause at least $5,000 in loss. SER 21. Keys admitted this knowledge in the course of the email campaign. Writing as "Fox Mulder," Keys held forth at length about how an investigation to identify computer intruders is "a long and painstaking process." SER

775-76. Keys's periodic taunting also demonstrated that, for his part, Keys wanted to cause alarm and an expensive response. *See* SER 773, 784, 796. This desire was relevant to the jury's determination that causing $5,000 in loss was within the scope of Keys's agreement. *See* SER 961.

Third, the email campaign was relevant to show motive. "Motive is evidence of the commission of any crime." *United States v. Bradshaw*, 690 F.2d 704, 708 (9th Cir. 1982). A rational jury could take the emails together with the other evidence and accept the government's theory of motive: Keys was an angry former employee who hated his bosses and used back door CMS passwords for revenge. SER 725. When Mercer wrote to "Fox Mulder" that FOX40 was made up of "good people," Keys responded that "good people" do not fire various employees including web producers. SER 770-74. "Walter Skinner" told viewers that FOX40's work "shriek[ed] of whoring out news and information rather than producing quality, hard-hitting journalism." SER 787-88.

Fourth, the emails were relevant to attribution of all the other conduct. The email campaign was used in the testimony of the FBI

summary witness who compared IP addresses, times, and activity on Keys's computer, the CMS, the Anonymous chatroom, and Overplay to attribute the conduct to Keys. SER 629-61, 574-694. The same IP address (80.74.135.87) was used to create the back-door super user account "anon1234" and to log into the Cancerman email accounts. SER 638-39, 840-49, 871. That IP address traced back to Overplay, which Keys used to hide his Sacramento IP and location.[6] SER 641-47, 83-89. Because the IP address used to log into the Cancerman email accounts was the same one used to construct a back door into the CMS, the email campaign helped show that the person who conducted the email campaign did the other things, and that person was Keys.

The emails were also relevant as Keys's own admissions that he retained the ability to log into the CMS after he left his employment. Keys sent the last email in the campaign on December 6. SER 787-

[6] Another Cancerman IP address figured in attribution: The evidence showed that a separate IP address, 91.214.168.172, also belonged to Overplay and was used by Keys to both log into the Cancerman email accounts, as well as change his successor's password. SER 658, 847 (CMS records), SER 871-882 (Yahoo! records), 883-89 (Overplay records).

88. In the campaign he had bragged about his ongoing CMS access. SER 787-88, 784, 786. The emails together tended to make it more likely that Keys was AESCracked, the person who, on December 8, gave CMS credentials to Anonymous and identified himself as a former employee. SER 807-12; *see United States v. Alvarez*, 358 F.3d 1194, 1205 (9th Cir. 2004) (defendant's possession of handheld radios relevant to show that he participated in narcotics conspiracy that had used the same model of handheld radios).

Finally, the emails were necessary to tell a coherent story that began with the newsroom argument and ended with the unsuccessful attempt to publishe a defaced *Los Angeles Times* front page. A jury is entitled to hear the background and context of a criminal charge because "[i]t cannot be expected to make its decision in a void—without knowledge of the time, place, and circumstances of the acts which form the basis of the charge." *United States v. Daly*, 974 F.2d 1215, 1217 (9th Cir. 1992) (quotations and citation omitted). Accordingly, a trial court may allow the prosecutor to offer evidence in order to provide "a coherent and comprehensible story regarding

the commission of the crime." *United States v. Beckman*, 298 F.3d 788, 794 (9th Cir. 2002).

The email campaign was an essential part of the story. Keys wrote emails that set the stage for his subsequent actions, evinced his motive, confessed his access to the CMS, showed his use of Overplay, initiated Tribune Company's response, and showed that Keys had not lost interest in Tribune Company in the time between his loss of employment and the attack on the *Los Angeles Times*. Keys confessed to the email campaign in the same written statement to the FBI. *See* SER 201 (audio). In light of these reasons, the district court acted well within its discretion when it overruled Keys's relevancy objection.

C. The court did not commit plain error in admitting Keys's other malicious conduct.

1. Locking Samantha Cohen out of the CMS

Keys sent particular commands to the CMS to repeatedly alter Cohen's credentials and lock her out of the CMS. SER 847, 487-89; 675-76. Keys did not object to any of this testimony. SER 847, 847-49, 675-76. This conduct impaired his replacement's access to the system, which she needed to do her job. *See* SER 837, 789-94; 528-

535. It was relevant for the jury to consider on the element of "damage," which includes any impairment to the availability of a system. *See* 18 U.S.C. § 1030(e)(8); *United States v. Middleton*, 231 F.3d 1207, 1209 (9th Cir. 2000) (damage from changing administrator passwords); *NovelPoster*, 140 F. Supp. 3d at 957, 961 (damage from changing plaintiff's password and thus preventing access to email accounts).

2. Creating Back Doors

Keys did not object when witnesses identified what command lines Keys used to create back doors. SER 473-77; 640-46. He did not object to testimony that explained what a back door was. SER 466, 473-74, 499-504, 603-05, 538-641, 647. He also did not object to Tribune Company employee testimony that it was an essential system function to ensure that only valid content was published on the web site. SER 455. It was not plain error to admit this evidence because it was relevant to whether Keys had damaged system integrity. This Court discussed similar conduct in *Middleton,* which was another CFAA case involving a defendant who altered network

logon credentials as part of a malicious campaign against his former employer. *See* 231 F.3d at 1208-9.

D. The probative value of Keys's emails and interference with Cohen's login credentials was not substantially outweighed by the danger of unfair prejudice.

Although Keys repeatedly asserts that the email and Cohen lockout evidence was "highly prejudicial," he never explains how jurors could be so inflamed as to render an improper verdict. "Unfair prejudice" means an "'undue tendency to suggest a decision on an improper basis, commonly, though not necessarily, an emotional one.'" *United States v. Hankey*, 203 F.3d 1160, 1172 (9th Cir. 2000) (quoting Fed. R. Evid. 403, Advisory Comm. Notes).

The three cases cited by Keys demonstrate the type of evidence that can be unfairly prejudicial and stand in stark contrast to this one. *See United States v. Layton*, 767 F.2d 549, 556 (9th Cir. 1985) (recording that captured infants crying and dying during the Jonestown mass murder/suicide); *United States v. Ellis*, 147 F.3d 1131, 1135-37 (texts about violence and the capabilities of explosives); *United States v. Bland*, 908 F.2d 471, 473 (9th Cir. 1990) (statement that defendant tortured and murdered a seven-year-old

girl). Keys's only argument is that the email campaign may have confused the jury because it ended a few days before the *Los Angeles Times* defacement, but, again, Keys ignores the broad time scope and narrative allegation in the indictment. *Compare* AOB at 39-40 *with* count 1, ¶ 1(h) (ER 236).

There was no unfair prejudice. Computer users do not like email spam or login issues, but these things lack the prejudicial effect of infanticide. In this case, the court examined the evidence and ordered the redaction of one of the emails to hide from the jury that the email campaign had terrified an elderly woman and reduced her to tears. *Compare* SER 777-80 *with* SER 976; SER 992-95. The court did not abuse its discretion.

III. The court's jury instruction on damage was correct.

A. The court instructed in the language of the statute.

The court instructed in the language of the CFAA, which defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). No elaboration on the statutory language was necessary because "these are common terms, whose meanings are within the

comprehension of the average juror." *United States v. Dixon*, 201 F.3d 1223, 1231 (9th Cir. 2000); *see also United States v. Young*, 458 F.3d 998, 1010 (9th Cir. 2006). A court's gloss on these words was not necessary. *Cf. Yoder & Frey Auctioneers, Inc.*, 774 F.3d at 1072 n.5 ("Integrity" refers to an "uncorrupted condition," an "original perfect state," and "soundness" while "impairment" means "deterioration" or "injurious lessening or weakening.").

B. The court properly denied Keys's requested instruction that backed-up data can never be damaged.

1. Standard of Review

Keys requested a jury instruction precluding a finding of "damage" to backed-up data. ER 166. This Court reviews the language and formulation of a jury instruction for an abuse of discretion. *United States v. Garcia*, 768 F.3d 822, 827 (9th Cir. 2014). A claim that an instruction misstated the law is reviewed de novo. *Id.* "In reviewing jury instructions, the relevant inquiry is whether the instructions as a whole are misleading or inadequate to guide the jury's deliberation." *Dixon*, 201 F.3d at 1230. "The trial court has substantial latitude so long as its instructions fairly and

adequately cover the issues presented." *United States v. Frega*, 179 F.3d 793, 806 n.16 (9th Cir. 1999).

2. Keys's proposed instruction contradicts the plain language of the statute.

Keys asserts that "it was error not to permit the Jury to consider whether the existence of previous versions of the latimes.com story meant there was no CFAA Damage." AOB at 35. Keys understates how far he wanted the district court to go in endorsing his theory. His submitted instruction was, "If the data was still available to the alleged victim, either because it was backed up or was elsewhere, there is not 'damage' under the CFAA." ER 166.

"While a defendant is entitled to an instruction that adequately addresses his theory of defense, he is not entitled to an instruction that misstates the law." *See United States v. George*, 420 F.3d 991, 1000 (9th Cir. 2005). The instruction misstated the law. The CFAA punishes any impairment to the availability of data or information. *See* 18 U.S.C. § 1030(e)(8). The evidence was that Keys and his co-conspirators impaired the availability of the original article to the readers of the *Los Angeles Times*. SER 377-81. A jury may find that

making a business's web service unavailable to its customers is CFAA damage. *See, e.g., Yoder & Frey Auctioneers, Inc.*, 774 F.3d at 1073 (impairing availability of customers' online bidding slots); *United States v. Schuster*, 467 F.3d 614, 615 (impairing availability of customers' internet connection).

Keys was able to argue his backed-up-data theory in his closing:

> So let's talk about what damage is, and I think this is from the actual jury instruction. I'll be corrected if I'm wrong. It's any impairment to the integrity or availability of data, program, system, or information.
>
> The system wasn't hurt. The information wasn't hurt. There was a back-up. The integrity or the availability of data wasn't hurt.
>
> . . .
>
> This is our argument on damage. If the data was still available to the complaining witness . . . either because it was backed up or elsewhere, there is not damage within the meaning of this case.

SER 762-63, 409-11. The jury was free to evaluate this in light of the testimony that the mobile version of the defaced story was up for a day and could not simply be restored with the press of a button. SER

380. At any rate, Keys was not entitled to have the court instruct the jury that Keys was right.

Keys cites to a handful of district court opinions outside the Ninth Circuit to argue that his iteration of the jury instruction was warranted. *See* AOB at 35 (citing *Instant Tech., LLC v. DeFazio*, 40 F. Supp. 3d 989, 1019 (N.D. Ill. 2014); *Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc.*, No. 1:10-CV-450, 2012 WL 2524008, at *6 (W.D. Mich. June 29, 2012); *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-1029, 2011 WL 4467767, at *8 (E.D. Pa. Sept. 23, 2011); *Cheney v. IPD Analytics, L.L.C.*, No. 08-23188-CIV, 2009 WL 1298405, at *6 (S.D. Fla. Apr. 16, 2009)). Those cases are distinguishable. None of them involved making information on a public website unavailable to its readers. They offer no insight into how the CFAA reaches the unauthorized alteration of an article in a news site.

The rule of lenity has no import merely because Keys's argument has not yet been presented to this Court. AOB at 36.

> While no previous Ninth Circuit case has addressed this particular issue, that is not determinative . A lack of prior appellate rulings on the topic does not render the law vague. The rule of lenity only applies . . . where there is a grievous ambiguity or

> uncertainty in the language and structure of the statute, such that even after a court has seized every thing from which aid can be derived, it is still left with an ambiguous statute.

United States v. Wanland, 830 F.3d 947, 953-54 (9th Cir. 2016); *United States v. Banks*, 514 F.3d 959, 968 (9th Cir. 2008).

This Court looks at legislative intent before applying the rule of lenity. *See Moskal v. United States*, 498 U.S. 103, 108 (1990). In expanding the definition of "damage," Congress expressly wanted to cover conduct that covertly breaches a network, causing "system users to change their passwords" and "the system administrators to devote resources to re-securing the system." Sen. Rep. No. 104-357, at 11 (1996). That is exactly what happened in *Middleton*, an earlier former employee hacking case considered by this Court. *See* 231 F.3d at 1208-9. That is also exactly what happened in this case, when Tribune Company discovered that the CMS had been breached to obtain the FOX40 Rewards email list and, a few days later on a larger scale, when Tribune Company discovered the *Los Angeles Times* defacement. SER 795, 255-56, 392-94, 436, 455, 589, 617-18.

IV. The court did not err in denying Keys's motion for acquittal.

A. Standard of Review

This Court reviews de novo the district court's denial of a motion for judgment of acquittal based on insufficient evidence. *See United States v. Mincoff*, 574 F.3d 1186, 1191-92 (9th Cir. 2009). This Court only determines whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt. *See United States v. Nevils*, 598 F.3d 1158, 1163-64 (9th Cir. 2010) (en banc).

B. Count two was supported by a sufficient showing of at least $5,000 in loss.

Nevils defeats Keys's attack on the strength of the evidence of loss in this case. Viewing the evidence in the light most favorable to the prosecution, a rational trier of fact could have found there was at least $5,000 in loss. *Nevils*, 598 F.3d at 1164. This Court has already approved calculating loss in terms of the monetary value of responding employee time. *See Middleton*, 231 F.3d at 1213-14. The jury was entitled to credit the ten employees of the Tribune Company who testified about their salary and the number of hours they

personally spent responding to Keys's course of conduct. SER 282-89, 350-60, 384-95, 411-12, 442-54, 462-66, 494, 497, 502-04, 546-48, 609-10, 700-04.

Keys does not contend that the court erred by allowing these percipient witness to offer opinions about the work that they did. SER 185-86; s*ee Tampa Bay Shipbuilding & Repair Co. v. Cedar Shipping Co.*, 320 F.3d 1213, 1223 (11th Cir. 2003); *see* Fed. R. Evid. 701, 2000 advisory comm. note. He merely argues here that the government's proof was unsupported by expert testimony. AOB 38. He made the same argument to the jury. SER 764. But the jury convicted. This Court must presume that the jury concluded that the witnesses were accurate that their time spent was reasonably related to the attack and this Court "must defer" to the jury's conclusion. *Nevils*, 598 F.3d at 1164. What matters is that Keys does not, and cannot on this record, contend that it was irrational to find that loss exceeded $5,000. *Id.*

Keys argues that CFAA loss does not include business losses or other lost revenue. AOB at 37. Keys cites nowhere in the trial record where business or revenue loss evidence was presented. The

government in closings only relied on the value of employee time spent. SER 743-45, 765-69. Keys's lost revenue argument is irrelevant to this appeal.

C. A rational jury could have found that Keys intended to and did take a substantial step toward damaging the Tribune Company's CMS by posting an entire defaced front-page newspaper layout.

To establish attempt, the evidence must show that the defendant intended to commit the crime charged and that he took a substantial step toward committing that crime. *United States v. Goetzke*, 494 F.3d 1231, 1235 (9th Cir. 2007). A rational jury could have found that the defendant knew what Sharpie intended and did his best to help. Keys can be liable either as a principal and an aider and abettor. *See Rosemond v. United States*, 134 S. Ct. 1240, 1249, (2014). Keys is responsible not only for his own substantial steps, but for the person whom he assisted. *Id.*

There was more than sufficient evidence of Keys's intent to cause damage. In the chatroom, Keys encouraged his co-conspirators to deface the Tribune Company's "bread and butter assets" and emphasized why he provided his co-conspirators with passwords to

the CMS. *See* SER 810, 863 ("[I] did not give you those passwords for 'research.' [I] want you to fuck shit up."). When Keys saw the defaced news story, he felt like he had incited it. SER 823 (audio). In the chatroom, when Sharpie told Keys that he had successfully defaced a story and had "a whole front page layout" that he was unable to post, Keys showed his intent in trying to help Sharpie. SER 856.

There was also ample evidence for a rational jury to find that Keys and Sharpie took a substantial step toward posting the defaced front page on the CMS. "A substantial step is an 'appreciable fragment' of a crime, an action of 'such substantiality that, unless frustrated, the crime would have occurred.'" *United States v. Nelson*, 66 F.3d 1036, 1042 (9th Cir. 1995) (quoting *United States v. Buffington*, 815 F.2d 1292, 1303 (9th Cir. 1987)).

When Keys told Sharpie that he was trying to re-enter the system, Keys was actually transmitting commands to the Tribune CMS. SER 853, 857, 857, 686-91. The jury could rationally find that they together had taken a substantial step toward committing that crime. Keys's attempted logins only failed because Tribune Company

had, in essence, changed the locks. This was sufficient to "cross the line between preparation and attempt by unequivocally demonstrating that the crime [would] take place unless interrupted by independent circumstances." *United States v. Goetzke*, 494 F.3d 1231, 1237 (9th Cir. 2007).

Keys and his co-conspirators' efforts to log into the CMS to deface the paper are analytically similar to actual movement – the turning of a key. Their conduct went beyond mere preparation. *See United States v. Moore*, 921 F.2d 207, 209 (9th Cir. 1990) (finding a substantial step where defendant was "walking toward the bank, wearing a ski mask, and carrying gloves, pillowcases and a concealed, loaded gun"). These actual log-in attempts with erstwhile valid passwords distinguish the authority invoked by Keys. *See* AOB at 44 (citing *United States v. Still*, 850 F.2d 607, 609 (9th Cir. 1988)). In *Still*, this Court held that preparing disguises and weapons was not a substantial step toward committing bank robbery. *Still* reasoned that the would-be bank robber did not cross the line from preparation to attempt because there was no "actual movement toward the bank or actions that [were] analytically similar to such

movement." *Still*, 850 F.2d at 610; *see also United States v. Harper*, 33 F.3d 1143, 1147 (9th Cir. 1994).

By analogy, in this case Keys and his confederate had prepared a robbery kit and tried to enter the bank by using a key that had worked the day before. A rational jury could conclude that he and Sharpie only failed because the bank had changed the locks. Absent this independent circumstance, Keys and his co-conspirators would have completed their crime. Viewed in the light most favorable to the government, a rational jury could have found that Keys took a substantial step toward damaging the Tribune Company's CMS. Hence, it was proper for the district court to deny Keys's motion for acquittal.

V. The court did not abuse its discretion by ordering restitution

A. Standard of Review

Keys objected to the restitution order. "The legality of an order of restitution is reviewed de novo, and factual findings supporting the order are reviewed for clear error. Provided that it is within the bounds of the statutory framework, a restitution order is reviewed

for abuse of discretion." *See United States v. Brock-Davis*, 504 F.3d 991, 996 (9th Cir. 2007) (citations omitted).

B. An estimate of the value of salaried employee time and replacement value of a customer list for a marketing program were proper bases for calculating restitution.

The court could not require Tribune Company to participate in restitution proceedings, 18 U.S.C. § 3664(g)(1), but nonetheless had to calculate an appropriate amount of restitution as a part of the sentence that a victim cannot waive. *See United States v. Edwards*, 595 F.3d 1004, 1014 (9th Cir. 2010).

The court did not clearly err in using time estimates and salary to calculate restitution loss. The trial evidence made clear that Tribune Company's response was done in-house, involved far more people than testified, and that these salaried employees did not typically log their time. SER 293-98, 334-35, 802-04 (FOX40 personnel only); 605-12 (Tribune Company IT). The government's loss estimates were based on salary alone, but Tribune Company also paid its employees salary, health insurance, and 401(k) benefits, worth about 30% of their salaries. SER 289-90, 360, 412, 745. In light of that testimony and the U.S. Bureau of Labor Statistics'

report that private industry compensation is about 70% salary and 30% benefits, the court did not clearly err against Keys in accepting the $49,956 estimate of the value of lost employee time.

The destruction of the FOX40 Rewards program, administered through Greenlinks, was supported by trial evidence. SER 298, 802-04. Keys's emails seemed directed to destroying viewer confidence in this program – he invited viewers to ask if FOX40 was spying on them and their credit card statements. SER 783. Viewers called the station in panic about the security of their bank accounts and credit cards. SER 331-32.

The largest component of restitution was FOX40's $200,000 estimate for the effect that the email campaign had on the FOX40 Rewards program. The court did not accept the estimate that Del Core gave for the lost ratings and revenue when this program collapsed. Rather, it valued the list at its replacement cost of $10 per customer. This Court recently approved use of replacement value as a basis to value an asset in restitution proceedings. *See United States v. Kaplan*, 2016 WL 5859856, at *2 (9th Cir. Oct. 7, 2016). The $200,000 amount was supported by the statement of Jerry Del

Core, a witness who testified at trial and whose credibility as a person the court had opportunity to evaluate. SER 997-98, 695-708.

It does not matter that Keys never deleted FOX40's list of customers. When Keys was finished, it was a list of viewers so hostile to FOX40 that 95% of them terminated their membership. Keys accomplished his objective of making them distrust the FOX40 Rewards program. SER 992-95. The trial testimony, and common sense, was ample reason to credit Del Core's statement that "[w]hen the database was compromised people canceled their participation." SER 997-98. Further, "[a]fter the compromise, FOX40, had to rebuild the database. Out of the original 20,000 accounts in the database, only 1,000 were retained as the database had to start anew. It took three years to build it back up to its prior level." SER 997-98.

CONCLUSION

The government respectfully requests that this Court affirm Keys's convictions and sentences on the two challenged counts, and the restitution order.

Respectfully submitted,

PHILLIP A. TALBERT
Acting United States Attorney

/s/ Matthew D. Segal
MATTHEW D. SEGAL
Assistant United States Attorney

STATEMENT OF RELATED CASES

The government is not aware of any related cases.

CERTIFICATE OF COMPLIANCE

Pursuant to Ninth Circuit Rule 32(a)(5)(A), I certify that the Answering Brief of the United States is proportionately spaced, has a typeface of 14 points or more, and contains 12,819 words.

DATED: November 18, 2016

/s/ Matthew D. Segal
MATTHEW D. SEGAL
Assistant United States Attorney

CERTIFICATE OF SERVICE

When All Case Participants are Registered for the
Appellate CM/ECF System

I hereby certify that on November 18, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

/s/ Matthew D. Segal
MATTHEW D. SEGAL
Assistant United States Attorney