A DIFFERENT UBER POST-MORTEM

Joe Sullivan
CEO of Ukraine Friends, he/him

War Stories - On the Record @Harrahs
joesullivansecurity.com
ukrainefriends.org

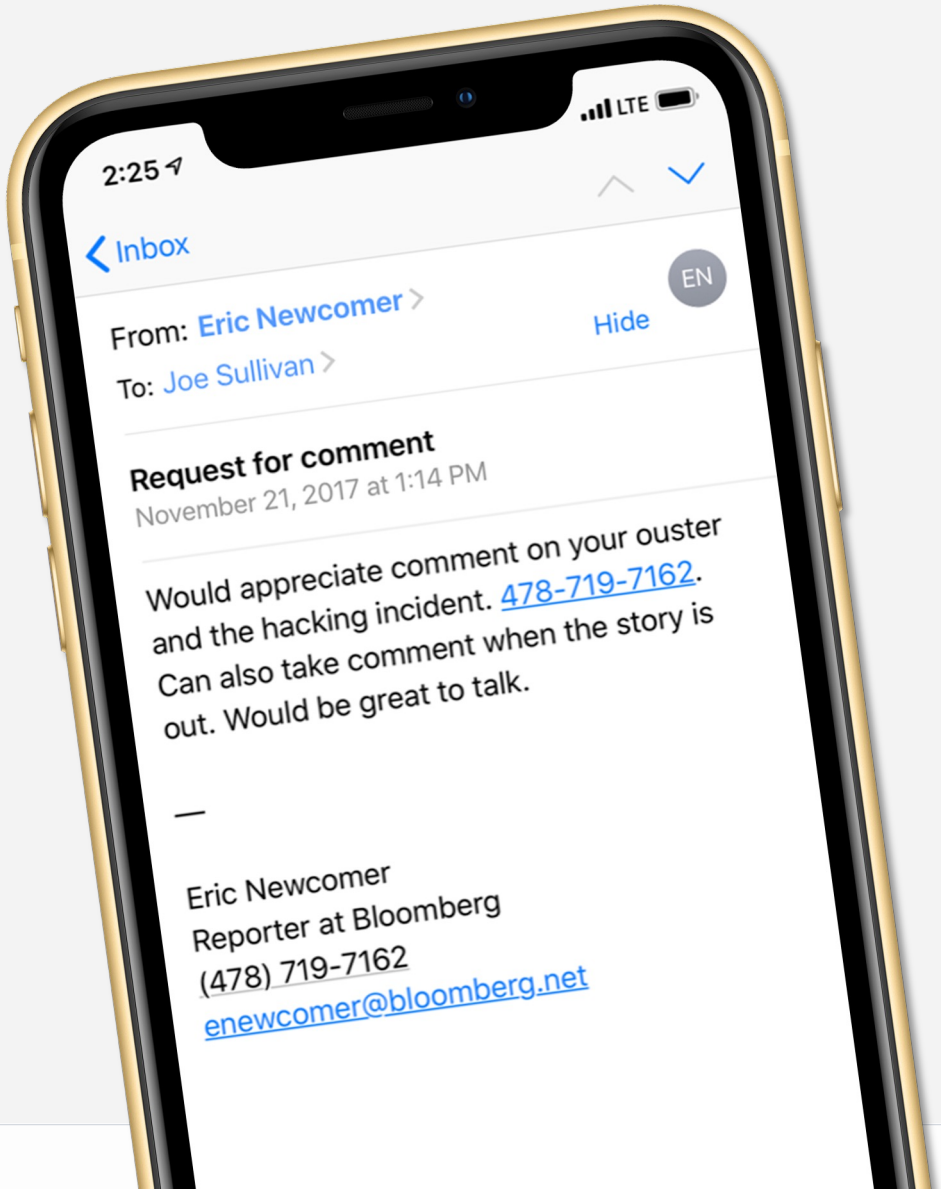
August 2023



SPEAKER BIO

- 2023 - Present — Ukraine Friends CEO
- 2018 - 2022 — Cloudflare CSO
- 2015 - 2017 — Uber CSO
- 2016 — Obama Presidential Commission on Cybersecurity
- 2008 - 2015 — Facebook CSO
- 2002 - 2008 — eBay / Paypal
- 1993 - 2002 — U.S. Department of Justice

Nov 2017


2:25
LTE
Inbox
From: Eric Newcomer
To: Joe Sullivan
Hide
EN
Request for comment
November 21, 2017 at 1:14 PM
Would appreciate comment on your ouster and the hacking incident. 478-719-7162. Can also take comment when the story is out. Would be great to talk.
—
Eric Newcomer
Reporter at Bloomberg
(478) 719-7162
enewcomer@bloomberg.net

Nov 2017

News

THE WALL STREET JOURNAL.

TECH

Uber Reveals Data Breach and Cover-up, Leading to Two Firings

Ride-hailing company says it will notify affected account holders in the coming days



By Greg Bensinger and Robert McMillan

November 21, 2017, 11:38 pm ET

Uber Technologies Inc. on Tuesday revealed it paid hackers $100,000 in an effort to conceal a data breach affecting 57 million accounts one year ago, a disclosure that adds to a string of scandals and legal prob-

Bloomberg US Ed

Live Now Markets Economics Industries Tech AI Politics Wealth Pursuits Opinion Businessweek Equality Gr

Technology
Cybersecurity

Uber Paid Hackers to Delete Stolen Data on 57 Million People

- Company paid hackers $100,000 to delete info, keep quiet
- Chief Security Officer Joe Sullivan and another exec ousted



Uber Paid Hackers to Keep Massive Cyberattack Quiet

Gift this article

By Eric Newcomer
November 21, 2017 at 4:58 PM EST
Updated on November 21, 2017 at 10:21 PM EST

Nov 2017

Greg Ferro aka 'Etherealmind'
@etherealmind
Follow

Replying to @etherealmind @riskybusiness

"Uber's own board is now looking at Sullivan's team, with the help of an outside law firm." They were investigating the security team.

Link: Uber Pushed the Limits of the Law. Now Comes the Reckoning - Bloomberg -



Uber Pushed the Limits of the Law. Now Comes the Reckoning
The ride-hailing company faces at least five U.S. probes, two more than previously reported, and the new CEO will need to dig the company out of trouble.
bloomberg.com

3:18 AM - 23 Nov 2017

1 Retweet

Techmeme
@Techmeme
Follow

Sources: Kalanick and CSO Joe Sullivan ordered $100K ransom to be paid; Uber tracked the hackers, pushed them to sign NDAs, disguised the payment as bug bounty (New York Times)

nytimes.com/2017/11/21/tec...



Sources: Kalanick and CSO Joe Sullivan ordered $100K ran...
New York Times: Sources: Kalanick and CSO Joe Sullivan ordered $100K ransom to be paid; Uber tracked the hackers, pushed them to sign NDAs, disguised the payment as bug bou...
techmeme.com

7:01 PM - 21 Nov 2017

32 Retweets 34 Likes

Mike Houston
@WhiteHatGuy
Follow

Mueller placed his patsy Joseph E. Sullivan at Cloudflare to fix the 2018 midterm elections.

Sullivan tried to cover up the loss of 57 million Uber customer data records, was fired, then rehired by Cloudflare that controls FL, OH election encryption keys. americans4innovation.blogspot.com/2018/11/robert...

6:26 PM - 17 Nov 2018

3 Retweets 4 Likes

granick
@granick
Follow

I'm very curious about Joe Sullivan's story. He's got lots of experience and respectable credentials. He didn't need to risk his career and reputation on appeasing Uber overlords. So what happened?

10:07 AM - 22 Nov 2017

17 Likes

Mark Pesce
@mpesce
Follow

"former Uber CEO Travis Kalanick and ex-CSO Joe Sullivan oversaw the $100k payment to hackers, according to sources for The New York Times"

so that looks like a felony to me...?

10:04 PM - 22 Nov 2017

7 Retweets 19 Likes

Kumar
@datarade
Follow

"Uber is now the target of at least three potential class action lawsuits, at least five state attorney general investigations, and an inquiry by the FTC because of Sullivan's decision to pay off hackers and the cover ups."

via

@adamscrabble

1:36 PM - 19 Mar 2018

Nov 2017

AUG 2020

FBI San Francisco
San Francisco Media Office
media.sf@fbi.gov

August 20, 2020

FBI Statement on the Arrest of Former Uber CSO for Covering Up 2016 Hack

Transcript / Visit Video Source (https://www.fbi.gov/video-repository/fbi-statement-on-the-arrest-of-former-uber-cso-for-covering-up-2016-hack/view)

Hello, I am Craig Fair, the deputy special agent in charge of the FBI San Francisco Division.

The FBI is committed to working with private sector companies in order to assist in preventing a breach and dealing with the aftermath of a breach. Of course, prevention is the preferred method of countering the loss of data and private information.

It is only through a coordinated public-private partnership that we are able to assist companies whose databases have been compromised. It is alleged that rather than report the breach openly and honestly, so that we could assist Uber, Mr. Sullivan decided instead to mislead authorities by withholding information and attempting to cover his tracks. This decision ultimately made a bad situation worse and led to the charges that were unsealed today alleging Mr. Sullivan's crimes.

Nov 2017 **AUG 2020**

UNITED STATES DISTRICT COURT

for the

Northern District of California

FILED

Aug 20 2020

SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

United States of America
v.
JOSEPH SULLIVAN

Case No. 3-20-71168 JCS

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of Nov. 15, 2016 to Nov. 21, 2017 in the county of San Francisco and elsewhere in the Northern District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1505	Count One: Obstruction of Justice Max. Penalties: 5 years in prison; $250,000 fine; 3 years of supervised release; $100 special assessment; restitution; forfeiture
18 U.S.C. § 4	Count Two: Misprision of a Felony Max. Penalties: 3 years in prison; $250,000 fine; 1 year of supervised release; $100 special assessment; restitution; forfeiture

Nov 2017 AUG 2020 **Sept 2022**



Nov 2017 | AUG 2020 | Sept 2022 | **May 2023**

UNITED STATES OF AMERICA,) CR-20-00337 WHO
)
PLAINTIFF,) SAN FRANCISCO, CALIFORNIA
)
VS.) MAY 4, 2023
)
JOSEPH SULLIVAN,) PAGES 1-45
)
DEFENDANT.)

TRANSC
BEFORE THE H
UNITED

THE COURT: I

BUT ULTIMATELY, IF

BACK, IT WAS A VERY SUC

FOR WHATEVER REASON, TH

UP.

MR. DAWSON: A

EXCLUDED THE EVIDENCE FROM TRIAL, BUT THE HACKERS DID LIE TO UBER'S REPRESENTATIVES ABOUT WHAT THEY HAD DONE WITH THE DATA, AND THERE WAS AN ADDITIONAL INDIVIDUAL WHO HAD POSSESSION OF IT THAT UBER WAS UNAWARE OF.

THE COURT: BUT IT HADN'T BEEN EXPOSED.

MR. DAWSON: THAT IS TRUE.

AND I THINK IT'S IMPORTANT, WE ARE NOT CASTIGATING OR PASSING JUDGMENT ON THE TECHNICAL ASPECT.

THE COURT: BUT IT HADN'T BEEN EXPOSED.

MR. DAWSON: THAT IS TRUE.

AND I THINK IT'S IMPORTANT, WE ARE NOT CASTIGATING OR PASSING JUDGMENT ON THE TECHNICAL ASPECT.

COMPANIES / GOVERNMENT / RESEARCHERS

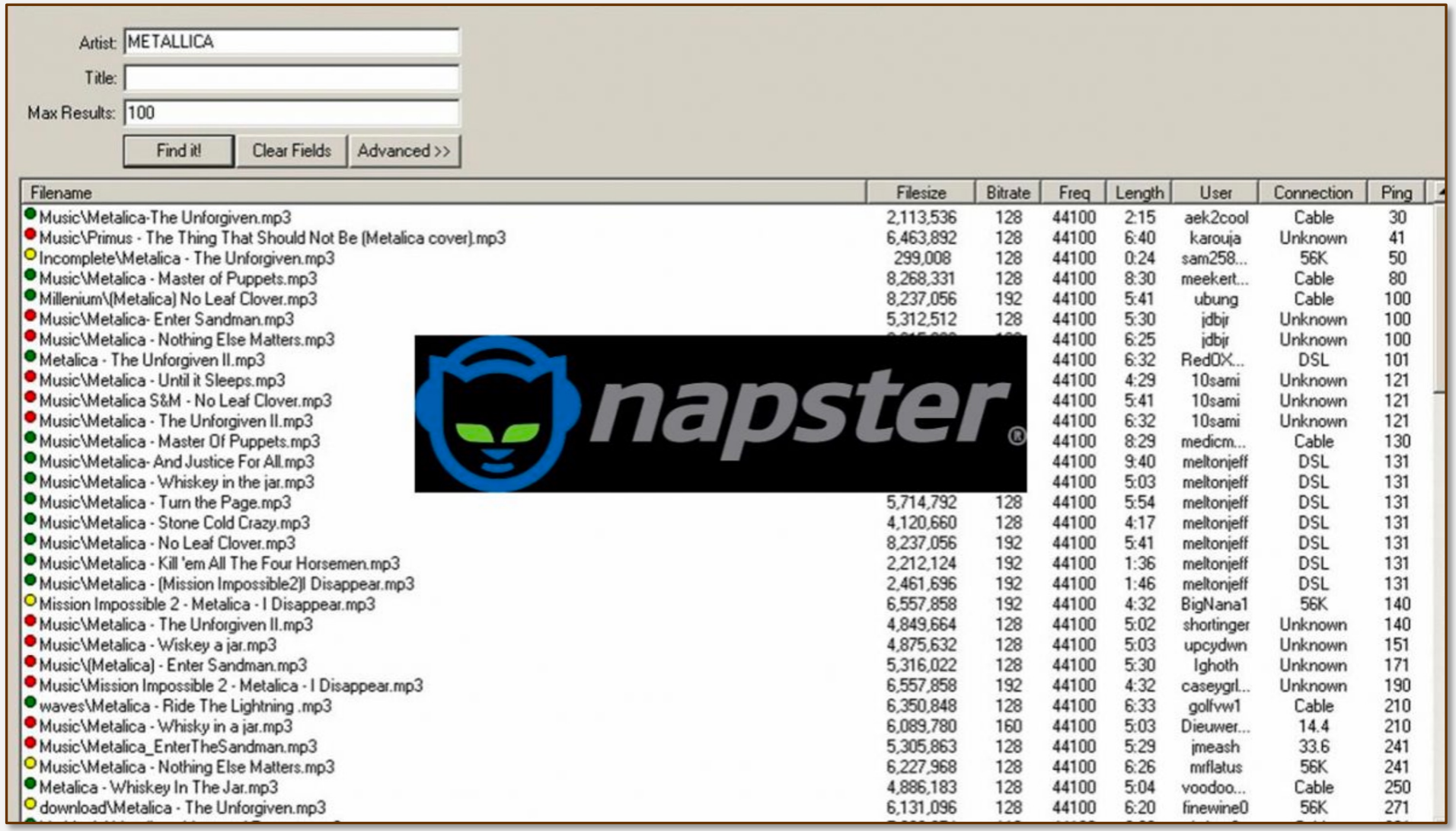
These three groups have been in collaborative tension for my entire professional life. This case highlights some major challenges that are still unresolved.

1. How do we tilt the bias against perceiving every request for payment as an attempt at extortion (especially in a world where ransomware is so prevalent)?
2. How do we protect an ecosystem where companies can leverage a researcher community to better protect themselves, and reduce their risks?
3. What can we do to help researchers trust a commitment from a company that they will not refer the researcher for prosecution?
4. How do we make sure that the law protects this engagement, allowing companies to utilize security researchers by authorizing access in a way that the government will respect?

Let's go way back in the timeline…



June 1999



Filename	Filesize	Bitrate	Freq	Length	User	Connection	Ping
Music\Metalica-The Unforgiven.mp3	2,113,536	128	44100	2:15	aek2cool	Cable	30
Music\Primus - The Thing That Should Not Be (Metalica cover).mp3	6,463,892	128	44100	6:40	karouja	Unknown	41
Incomplete\Metalica - The Unforgiven.mp3	299,008	128	44100	0:24	sam258...	56K	50
Music\Metalica - Master of Puppets.mp3	8,268,331	128	44100	8:30	meekert...	Cable	80
Millenium\(Metalica) No Leaf Clover.mp3	8,237,056	192	44100	5:41	ubung	Cable	100
Music\Metalica- Enter Sandman.mp3	5,312,512	128	44100	5:30	jdbjr	Unknown	100
Music\Metalica - Nothing Else Matters.mp3			44100	6:25	jdbjr	Unknown	100
Metalica - The Unforgiven II.mp3			44100	6:32	RedOX...	DSL	101
Music\Metalica - Until it Sleeps.mp3			44100	4:29	10sami	Unknown	121
Music\Metalica S&M - No Leaf Clover.mp3			44100	5:41	10sami	Unknown	121
Music\Metalica - The Unforgiven II.mp3			44100	6:32	10sami	Unknown	121
Music\Metalica - Master Of Puppets.mp3			44100	8:29	medicm...	Cable	130
Music\Metalica- And Justice For All.mp3			44100	9:40	meltonjeff	DSL	131
Music\Metalica - Whiskey in the jar.mp3			44100	5:03	meltonjeff	DSL	131
Music\Metalica - Turn the Page.mp3	5,714,792	128	44100	5:54	meltonjeff	DSL	131
Music\Metalica - Stone Cold Crazy.mp3	4,120,660	128	44100	4:17	meltonjeff	DSL	131
Music\Metalica - No Leaf Clover.mp3	8,237,056	192	44100	5:41	meltonjeff	DSL	131
Music\Metalica - Kill 'em All The Four Horsemen.mp3	2,212,124	192	44100	1:36	meltonjeff	DSL	131
Music\Metalica - (Mission Impossible2)I Disappear.mp3	2,461,696	192	44100	1:46	meltonjeff	DSL	131
Mission Impossible 2 - Metalica - I Disappear.mp3	6,557,858	192	44100	4:32	BigNana1	56K	140
Music\Metalica - The Unforgiven II.mp3	4,849,664	128	44100	5:02	shortinger	Unknown	140
Music\Metalica - Wiskey a jar.mp3	4,875,632	128	44100	5:03	upcydwn	Unknown	151
Music\(Metalica) - Enter Sandman.mp3	5,316,022	128	44100	5:30	Ighoth	Unknown	171
Music\Mission Impossible 2 - Metalica - I Disappear.mp3	6,557,858	192	44100	4:32	caseygrl...	Unknown	190
waves\Metalica - Ride The Lightning .mp3	6,350,848	128	44100	6:33	golfvw1	Cable	210
Music\Metalica - Whisky in a jar.mp3	6,089,780	160	44100	5:03	Dieuwer...	14.4	210
Music\Metalica_EnterTheSandman.mp3	5,305,863	128	44100	5:29	jmeash	33.6	241
Music\Metalica - Nothing Else Matters.mp3	6,227,968	128	44100	6:26	mrflatus	56K	241
Metalica - Whiskey In The Jar.mp3	4,886,183	128	44100	5:04	voodoo...	Cable	250
download\Metalica - The Unforgiven.mp3	6,131,096	128	44100	6:20	finewine0	56K	271

239 F.3d 1004 (2001)

A&M Records, Inc., a corporation; Geffen Records, Inc., a corporation; Interscope Records; Sony Music Entertainment, Inc.; Mca Records, Inc.; Atlantic Recording Corp.; Island Records, Inc.; Motown Record Co.; Capitol Records, Inc., Plaintiffs-Appellees,

v.

Napster, Inc., Defendant-Appellant. Jerry Leiber, individually and doing business as, Jerry Leiber Music; Mike Stoller and Frank Music Corp., on behalf of themselves and all others similarly situated, Plaintiffs-Appellees,

v.

Napster, Inc., Defendant-Appellant.

Nos. 00-16401, 00-16403.

United States Court of Appeals, Ninth Circuit.

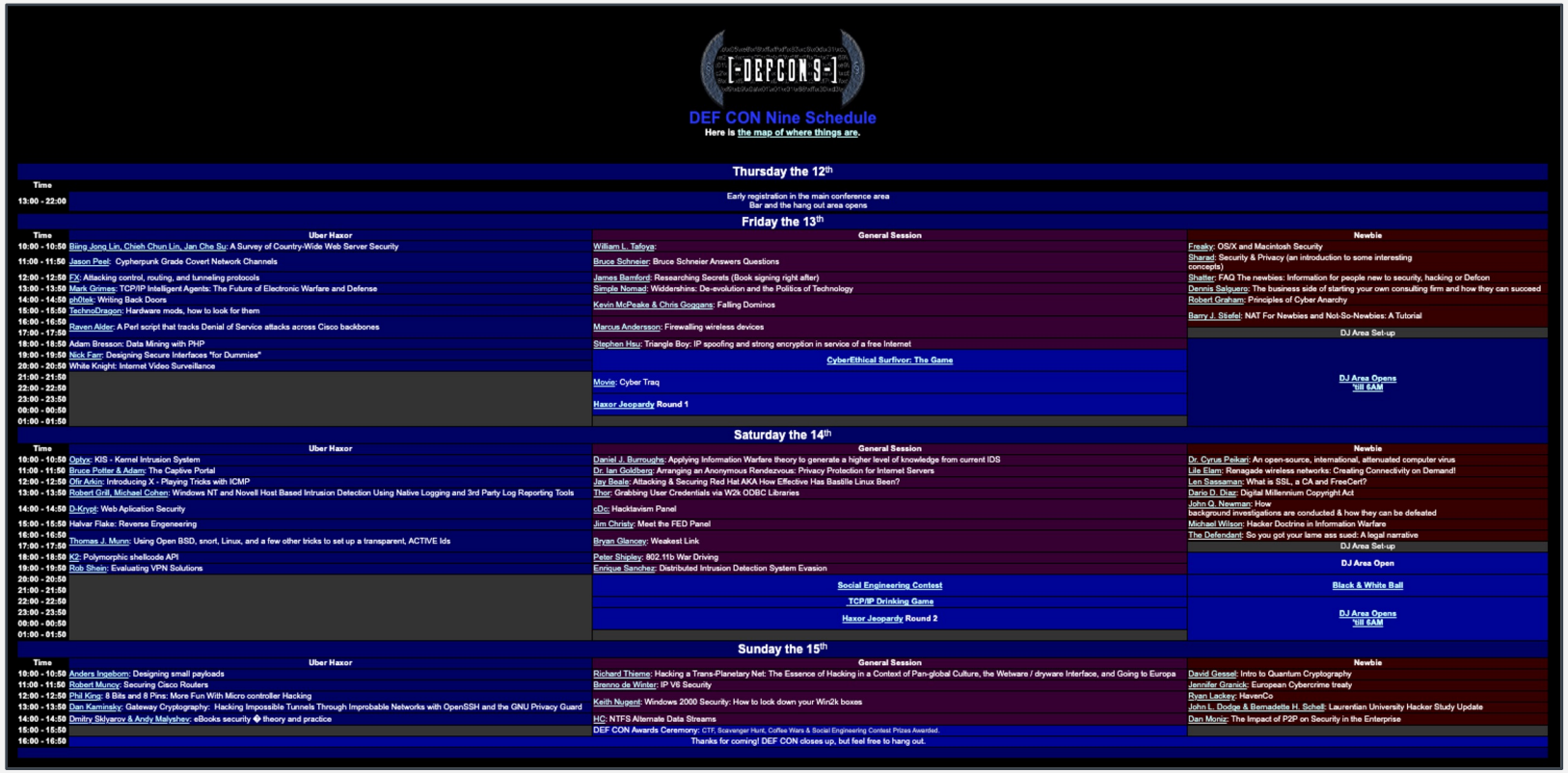
Argued and Submitted October 2, 2000.
Filed February 12, 2001.
As Amended April 3, 2001.



Notable incidents [edit source]

High-profile issues which have garnered significant media attention.

Year	Description
1999	On July 10, 1999, the Cult of the Dead Cow hacker collective released Back Orifice 2000 (later discovered to be infected with the CIH virus) at DEF CON 7, in what was, at the time, the largest presentation in DEF CON history.
2001	On July 16, 2001, Russian programmer Dmitry Sklyarov was arrested the day after DEF CON for writing software to decrypt Adobe's e-book format.



[-DEFCON 9-]

DEF CON Nine Schedule

Here is the map of where things are.

Thursday the 12th

Time	
13:00 - 22:00	Early registration in the main conference area Bar and the hang out area opens

Friday the 13th

Time	Uber Haxor	General Session	Newbie
10:00 - 10:50	Bing Jong Lin, Chieh Chun Lin, Jan Che Su: A Survey of Country-Wide Web Server Security	William L. Tafoya:	Freaky: OS/X and Macintosh Security
11:00 - 11:50	Jason Peel: Cypherpunk Grade Covert Network Channels	Bruce Schneier: Bruce Schneier Answers Questions	Sharad: Security & Privacy (an introduction to some interesting concepts)
12:00 - 12:50	FX: Attacking control, routing, and tunneling protocols	James Bamford: Researching Secrets (Book signing right after)	Shatter: FAQ The newbies: Information for people new to security, hacking or Defcon
13:00 - 13:50	Mark Grimes: TCP/IP Intelligent Agents: The Future of Electronic Warfare and Defense	Simple Nomad: Widdershins: De-evolution and the Politics of Technology	Dennis Salguero: The business side of starting your own consulting firm and how they can succeed
14:00 - 14:50	oh0tek: Writing Back Doors	Kevin McPeake & Chris Goggans: Falling Dominos	Robert Graham: Principles of Cyber Anarchy
15:00 - 15:50	TechnoDragon: Hardware mods, how to look for them		Barry J. Stiefel: NAT For Newbies and Not-So-Newbies: A Tutorial
16:00 - 16:50	Raven Alder: A Perl script that tracks Denial of Service attacks across Cisco backbones	Marcus Andersson: Firewalling wireless devices	
17:00 - 17:50			DJ Area Set-up
18:00 - 18:50	Adam Bresson: Data Mining with PHP	Stephen Hsu: Triangle Boy: IP spoofing and strong encryption in service of a free Internet	
19:00 - 19:50	Nick Farr: Designing Secure Interfaces "for Dummies"		
20:00 - 20:50	White Knight: Internet Video Surveillance	CyberEthical Surfivor: The Game	
21:00 - 21:50		Movie: Cyber Traq	DJ Area Opens 'till 6AM
22:00 - 22:50			
23:00 - 23:50		Haxor Jeopardy Round 1	
00:00 - 00:50			
01:00 - 01:50			

Saturday the 14th

Time	Uber Haxor	General Session	Newbie
10:00 - 10:50	Ophyx: KIS - Kernel Intrusion System	Daniel J. Burroughs: Applying Information Warfare theory to generate a higher level of knowledge from current IDS	Dr. Cyrus Peikari: An open-source, international, attenuated computer virus
11:00 - 11:50	Bruce Potter & Adam: The Captive Portal	Dr. Ian Goldberg: Arranging an Anonymous Rendezvous: Privacy Protection for Internet Servers	Lile Elam: Renagade wireless networks: Creating Connectivity on Demand!
12:00 - 12:50	Ofir Arkin: Introducing X - Playing Tricks with ICMP	Jay Beale: Attacking & Securing Red Hat AKA How Effective Has Bastille Linux Been?	Len Sassaman: What is SSL, a CA and FreeCert?
13:00 - 13:50	Robert Grill, Michael Cohen: Windows NT and Novell Host Based Intrusion Detection Using Native Logging and 3rd Party Log Reporting Tools	Thor: Grabbing User Credentials via W2k ODBC Libraries	Dario D. Diaz: Digital Millennium Copyright Act
14:00 - 14:50	D-Krypt: Web Aplication Security	cDc: Hacktavism Panel	John Q. Newman: How background investigations are conducted & how they can be defeated
15:00 - 15:50	Halvar Flake: Reverse Engeneering	Jim Christy: Meet the FED Panel	Michael Wilson: Hacker Doctrine in Information Warfare
16:00 - 16:50	Thomas J. Munn: Using Open BSD, snort, Linux, and a few other tricks to set up a transparent, ACTIVE Ids	Bryan Glancey: Weakest Link	The Defendant: So you got your lame ass sued: A legal narrative
17:00 - 17:50			DJ Area Set-up
18:00 - 18:50	K2: Polymorphic shellcode API	Peter Shipley: 802.11b War Driving	DJ Area Open
19:00 - 19:50	Rob Shein: Evaluating VPN Solutions	Enrique Sanchez: Distributed Intrusion Detection System Evasion	
20:00 - 20:50		Social Engineering Contest	Black & White Ball
21:00 - 21:50		TCP/IP Drinking Game	
22:00 - 22:50			DJ Area Opens 'till 6AM
23:00 - 23:50		Haxor Jeopardy Round 2	
00:00 - 00:50			
01:00 - 01:50			

Sunday the 15th

Time	Uber Haxor	General Session	Newbie
10:00 - 10:50	Anders Ingebom: Designing small payloads	Richard Thieme: Hacking a Trans-Planetary Net: The Essence of Hacking in a Context of Pan-global Culture, the Wetware / dryware Interface, and Going to Europa	David Gessel: Intro to Quantum Cryptography
11:00 - 11:50	Robert Muncy: Securing Cisco Routers	Brenno de Winter: IP V6 Security	Jennifer Granick: European Cybercrime treaty
12:00 - 12:50	Phil King: 8 Bits and 8 Pins: More Fun With Micro controller Hacking		Ryan Lackey: HavenCo
13:00 - 13:50	Dan Kaminsky: Gateway Cryptography: Hacking Impossible Tunnels Through Improbable Networks with OpenSSH and the GNU Privacy Guard	Keith Nugent: Windows 2000 Security: How to lock down your Win2k boxes	John L. Dodge & Bernadette H. Schell: Laurentian University Hacker Study Update
14:00 - 14:50	Dmitry Sklyarov & Andy Malyshev: eBooks security ◆ theory and practice	HC: NTFS Alternate Data Streams	Dan Moniz: The Impact of P2P on Security in the Enterprise
15:00 - 15:50		DEF CON Awards Ceremony: CTF, Scavenger Hunt, Coffee Wars & Social Engineering Contest Prizes Awarded.	
16:00 - 16:50		Thanks for coming! DEF CON closes up, but feel free to hang out.	

The Register

eBook security debunker arrested by Feds

Adobe kicks ass

John Leyden Mon 23 Jul 2001 // 12:01 UTC

A Russian security expert has been arrested after making a presentation at Defcon pointing out the shortcomings of eBook security.

Dmitry Sklyarov, of Russian software company ElcomSoft, and author of Advanced eBook Processor, which removes restrictions on reading and printing from encrypted PDF files, was arrested for alleged violations of the Digital Millennium Copyright Act.

According to an item on ElcomSoft's site, Sklyarov is being held a Las Vegas prison pending judgement on a motion filled by Adobe in California. Adobe has objected to the publication of the software and a presentation, entitled "eBook Security: Theory and Practice", that Sklyarov made at Defcon, the annual hacker's convention in Las Vegas.

SFGATE

July 31, 2001



Supporters of jailed Russian software programmer Dmitry Sklyarov, 26, carried protest signs outside the Federal Building in San Francisco yesterday, demanding dismissal of computer piracy charges against him. Chronicle photo by Vince Maggiora

Crypto-Gram

November 15, 2001

by Bruce Schneier
Founder and CTO
Counterpane Internet Security, Inc.
schneier@schneier.com
<http://www.counterpane.com>

A free monthly newsletter providing summaries, analyses, insights, and commentaries on computer security and cryptography.

Back issues are available at <http://www.schneier.com/crypto-gram.html>. To subscribe, visit <http://www.schneier.com/crypto-gram.html> or send a blank message to crypto-gram-subscribe@chaparraltree.com.

Copyright (c) 2001 by Counterpane Internet Security, Inc.

In this issue:

- Full Disclosure
- Crypto-Gram Reprints
- News
- Counterpane Internet Security News
- GOVNET
- Password Safe Vulnerability
- Microsoft on Windows XP
- Comments from Readers

Full Disclosure

Microsoft is leading the charge to restrict the free flow of computer security vulnerabilities. Last month Scott Culp, manager of the security response center at Microsoft, published an essay describing the current practice of publishing security vulnerabilities to be “information anarchy.” He claimed that we’d all be a lot safer if researchers would keep details about vulnerabilities to themselves, and stop arming hackers with offensive tools. Last week, at Microsoft’s Trusted Computing Forum, Culp announced a new coalition to put these ideas into practice.

June 1999 | Apr 2001 | July 2001 | Nov 2001 | **Nov 2007**

TUESDAY, NOVEMBER 20, 2007

PayPal's Vulnerability Disclosure Policy includes researcher protection

Update: 11.28.2007: Security Retentive, a PayPal employee who was personally involved with crafting the language of their disclosure policy, responds to public comments.

Update 11.21.2007: Kelly Jackson Higgins posted a sto
post.

Very few website owners post how security researche
them with regard to a discovered vulnerability. This s
most experts believe the vast majority of website cor
Microsoft, Yahoo, Google, and now Paypal have their
posted. The rest of the Alexa 500, if they have a post
extremely hard to find.

PayPal's newly posted vulnerability disclosure policy
be given special attention because they've done som
that and in my opinion very intelligent security-wise.
research follows their stated procedure, which is enti
PayPal states plainly that they'll not engage legal act
given the researcher confidence that nothing bad is g
to them as a result. I think this is first, and if not, I've

"To encourage responsible disclosure, we commit that - if we conclude that a disclosure respects and meets all the guidelines outlined below - we will not bring a private action or refer a matter for public inquiry."

This indicates that PayPal understands that security researchers are the good guys, but they are wary of disclosing website vulnerabilities to them for fear of legal issues. As a result researchers may choose to

ABOUT ME



Jeremiah Grossman

Jeremiah Grossman's career spans nearly 20 years and has lived a literal lifetime in

Yahoo!

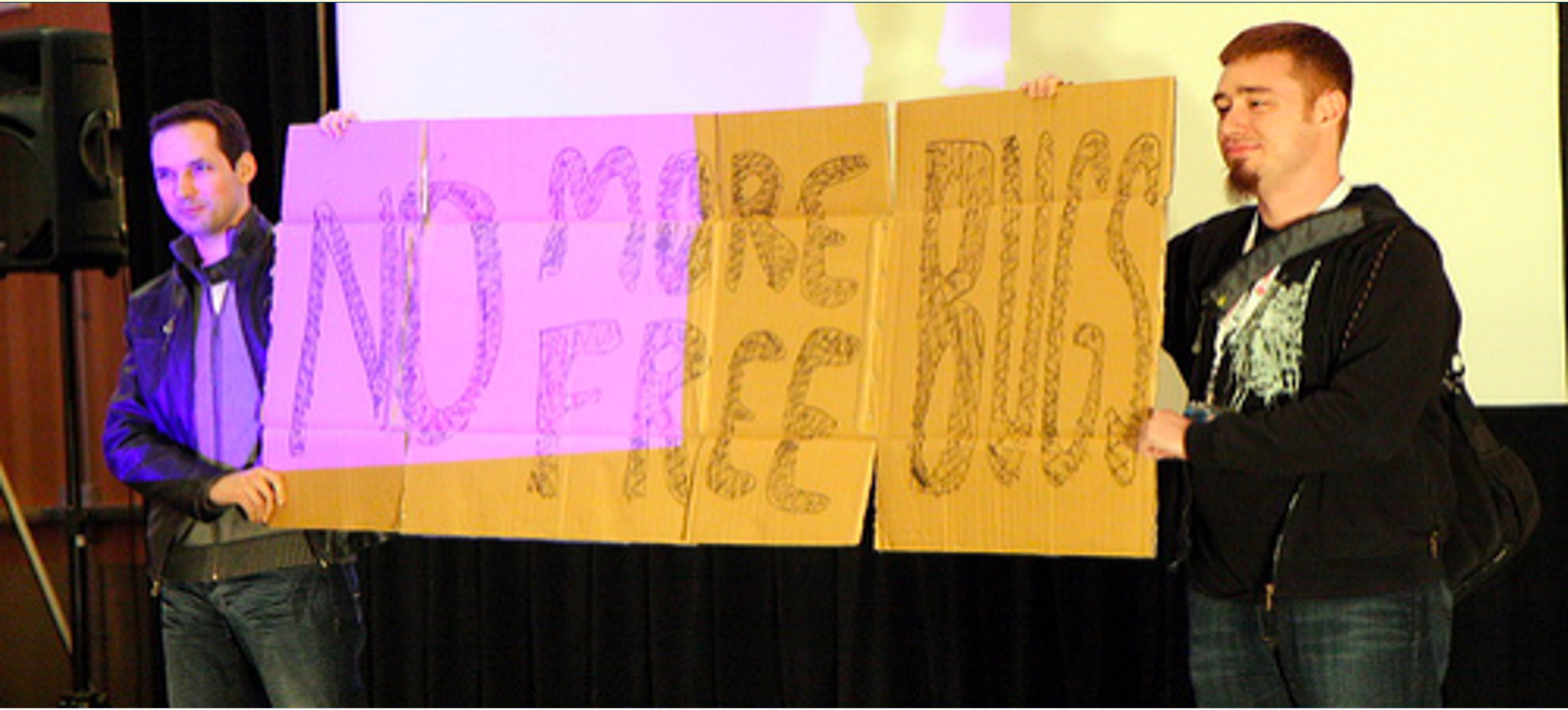
View my complete profile

LINKS

Jeremiah's Main Website
Twitter Profile
Facebook Profile
LinkedIn Profile

> "To encourage responsible disclosure, we commit that – if we conclude that a disclosure respects and meets all the guidelines outlined below - we will not bring a private action or refer a matter for public inquiry."

June 1999 | Apr 2001 | July 2001 | Nov 2001 | Nov 2007 | **Mar 2009**



Alex Sotirov & Dino Dai Zovi at CanSecWest

June 1999 | Apr 2001 | July 2001 | Nov 2001 | Nov 2007 | Mar 2009 | **Dec 2010**



ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

Knowledge is Power: Facebook's Exceptional Approach to Vulnerability Disclosure

BY MARCIA HOFMANN | DECEMBER 17, 2010

It's no surprise to EFF members that the Internet is full of security flaws, some of them severe. Yet many Internet companies try to deal with these problems internally, or not at all. They don't encourage outsiders to report flaws discovered when using or testing a website, and may even be hostile toward those who reveal facts they don't want to hear. Well-meaning Internet users are often afraid to tell companies about security flaws they've found — they don't know whether they'll get hearty thanks or slapped with a lawsuit or even criminal prosecution. This tension is unfortunate, because when companies learn what needs to be fixed, their services will be better and their users safer.

Facebook has set itself apart from other Internet companies by recognizing this problem and working to overcome it. The social networking site has become one of the first to publish a policy intended to make those who discover vulnerabilities more comfortable coming forward to report them:

"If you share details of a security issue with us and give us a reasonable period of time to respond to it before making it public, and in the course of that research made a good faith effort to avoid privacy violations, destruction of data, or interruption or degradation of our service, we will not bring any lawsuit against you or ask law enforcement to investigate you for that research."

What is Facebook doing at a hacker convention in Vegas? / The social network pays the underground a visit

By Adrianne Jeffries
Aug 2, 2013, 6:00 AM PDT | 0 Comments / 0 New





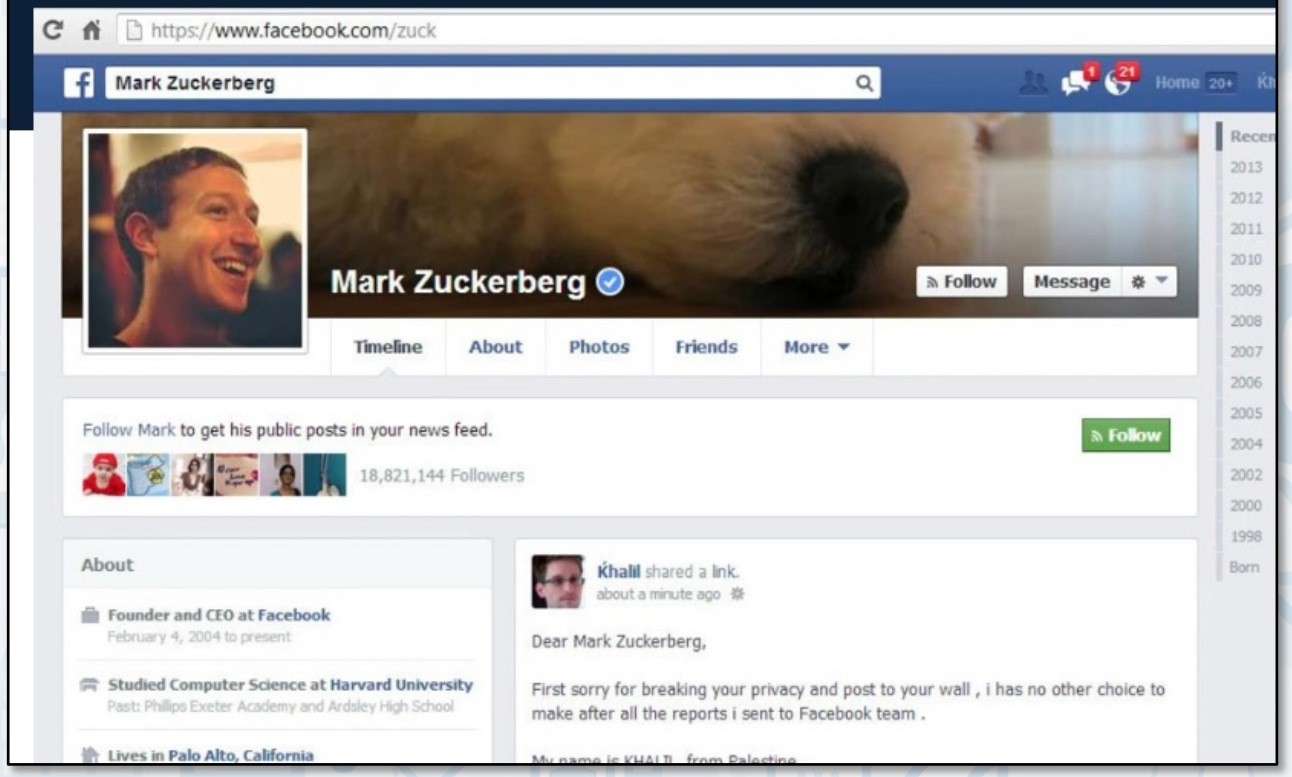
Facebook Offers Cash To 'Bug Bounty Hunters' At DefCon Hacker Conference

Facebook Offers Cash to 'Bug Bounty Hunters' at Hacker Conference

By Gerry Smith
Aug 6, 2011, 12:42 PM EDT | **Updated** Oct 6, 2011



One way to get Facebook's attention: Hack Zuckerberg's personal page



Hacker who exposed Facebook bug to get reward from unexpected source

Jim Finkle

3 MIN READ

BOSTON (Reuters) - A man who hacked into Mark Zuckerberg's Facebook page to expose a software bug is getting donations from hackers around the world after the company declined to pay him under a program that normally rewards people who report flaws.



Engineer nabs Facebook's biggest bug bounty yet, but not the jackpot he hoped for

By Jeremy Kirk
PCWorld | JAN 23, 2014 6:37 AM PST

Last November Reginaldo Silva, a computer engineer in Brazil, found one of the worst kinds of vulnerabilities in Facebook's software. It has netted him the biggest bug bounty the social network has ever paid out, but while he's not complaining, it wasn't quite the windfall he hoped for.

The bug related to code used for OpenID, an authentication system that lets people use the same login credentials for multiple online services.

Silva found that the vulnerability could be executed from a remote computer, one of the most dangerous types of software flaws. It could have allowed a hacker to read almost any file and open arbitrary network connections on a Facebook server.

"I knew I had found the keys to the kingdom," Silva wrote on his blog.

- 2013-11-23 7:54 pm: I sent an email explaining exactly how the attack could be escalated to an RCE (with file paths, example requests and all).
- 2013-11-24 9:23 pm: Facebook replied that my attack worked and they'd have to work around it.
- 2013-12-03 4:45 am: Facebook informed me that the longer term fix was in place and that they'd soon have a meeting to discuss a new bounty amount
- 2013-12-03 7:14 pm: I thanked them and said I'd cross my fingers
- 2013-12-13 1:04 pm: I found a Bloomberg article quoting Ryan McGeehan, who managed Facebook's incident response unit, saying that "If there's a million dollar bug, we will pay it out" and asked if there was any news.
- 2013-12-30 4:45 am: Facebook informed me that, since the bug was now considered to be RCE, the payout would be higher. I won't disclose the amount, but if you have any comments about how much you think this should be worth, please share them. Unfortunately, I didn't get even close to the one-million dollar payout cited above. In case you're wondering, I quoted Mr. McGeehan mostly as a joke.

June 2015

UBER

USER TERMS | PRIVACY | COPYRIGHT | SECURITY POLICY | OTHER

RESPONSIBLE DISCLOSURE POLICY

Maintaining the safety and privacy of your data with Uber is one of Uber Engineering's top goals. If you are a security researcher (or any other perceptive user) and have discovered a security vulnerability in one of our products, please contact security-abuse@uber.com. To report something particularly sensitive, you can use the Uber Product Security PGP/GPG Key to encrypt your email. We consider reports to this address to be of the highest priority, and will investigate them as quickly as possible.

For all other concerns, please visit help.uber.com or email support@uber.com.

For vulnerabilities reported to us in compliance with this disclosure policy, Uber commits to validate, respond to, and fix vulnerabilities in a timely fashion and to not take legal or administrative action against responsible vulnerability reporters. Uber reserves all of its legal rights in the event of noncompliance.

"Uber commits … to not take legal or administrative action against responsible vulnerability reporters"

June 2015



As a special thanks to individuals who have reported previously-unknown vulnerabilities of high or critical security, Uber will maintain a list of credits on this page.

ACKNOWLEDGEMENTS

- Rafael Pablos
- Arvind Singh Shekhawat
- Chetan Gulhane
- Nitin Goplani & Jatinder Pal Singh
- Manish Bhattacharya
- Dylan S Hailey
- Yuji Kosuga, PhD
- Tony Trummer & Tushar Dalvi
- Craig Young
- Martin Vigo
- Frans Rosén
- Jeffrey Rosen
- Evan Ricafort
- Rob Fletcher

June 2015 **Aug 2015**

UBER



Joe Sullivan

Worked at Uber (company) · Upvoted by Ryan McGeehan, Founding Advisor @ HackerOne, former Director @ FB Security / Coinbase Security and Michiel Prins, Co-Founder @ HackerOne · 8y ·

Originally Answered: Does Uber have a bug bounty program ? · Remove Banner

On the Uber Security Team, we want to foster strong relationships with the security community and love bug bounty programs. While we are still a very young company (just turned 5!), we have been actively engaging the community and working on rolling out a program formally.

Our responsible disclosure policy can be found at Uber. We also recognize reports in our Hall of Fame on the same page.

We have not launched a public bug bounty program yet, but we are running a beta program with HackerOne right now. Through that program a number of researchers have been giving us feedback. We've even steered specific researchers to the program.

Stay tuned for more details in the future.

1.2K views · View 20 upvotes

June 2015 Aug 2015 **Mar 2016**

Uber Newsroom

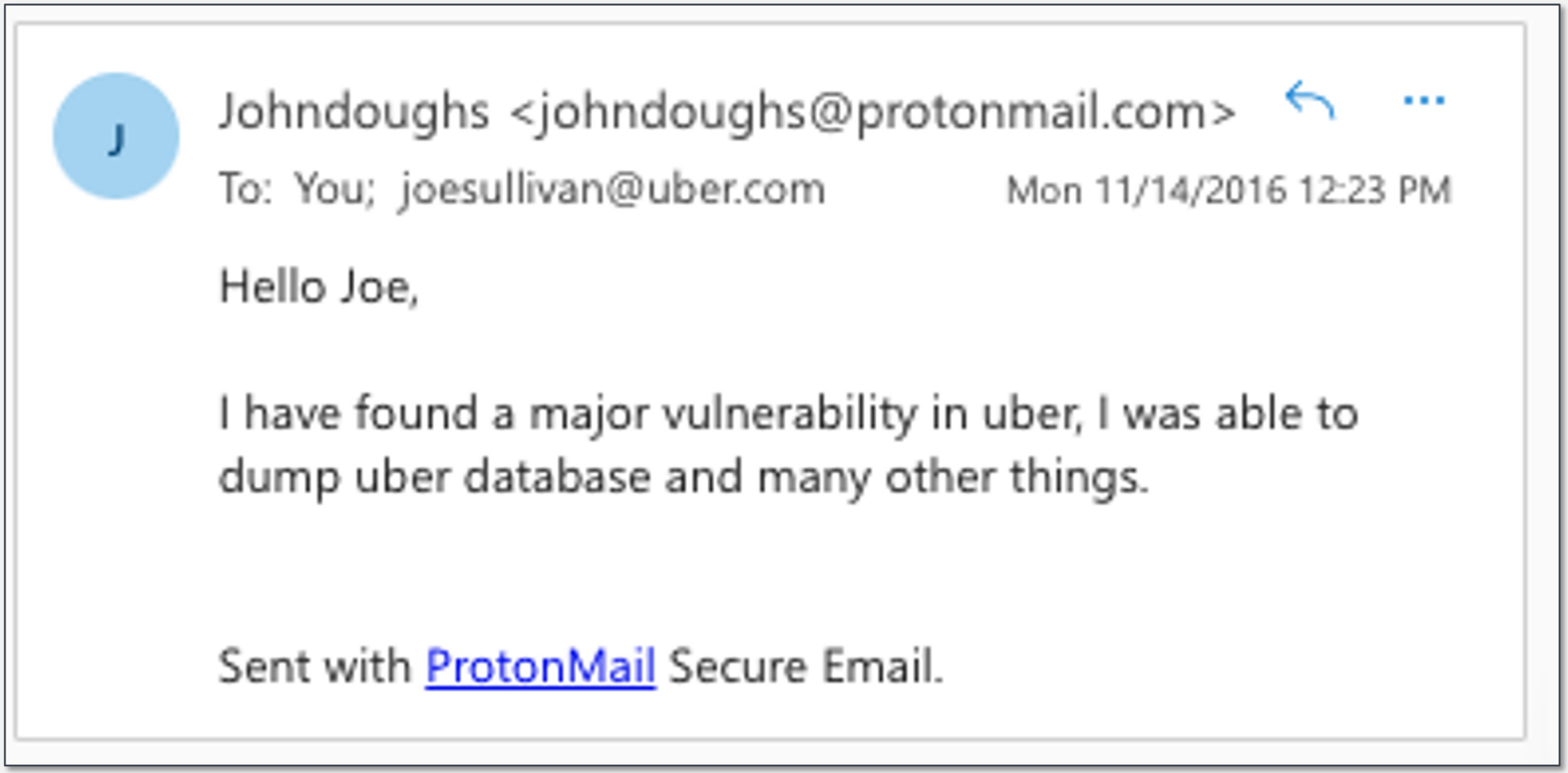
US | Mar 22, 2016

Welcome All Bug Bounty Hunters

Written by Sarah



June 2015 | Aug 2015 | Mar 2016 | **Nov 2016**



J

Johndoughs <johndoughs@protonmail.com>

To: You; joesullivan@uber.com Mon 11/14/2016 12:23 PM

Hello Joe,

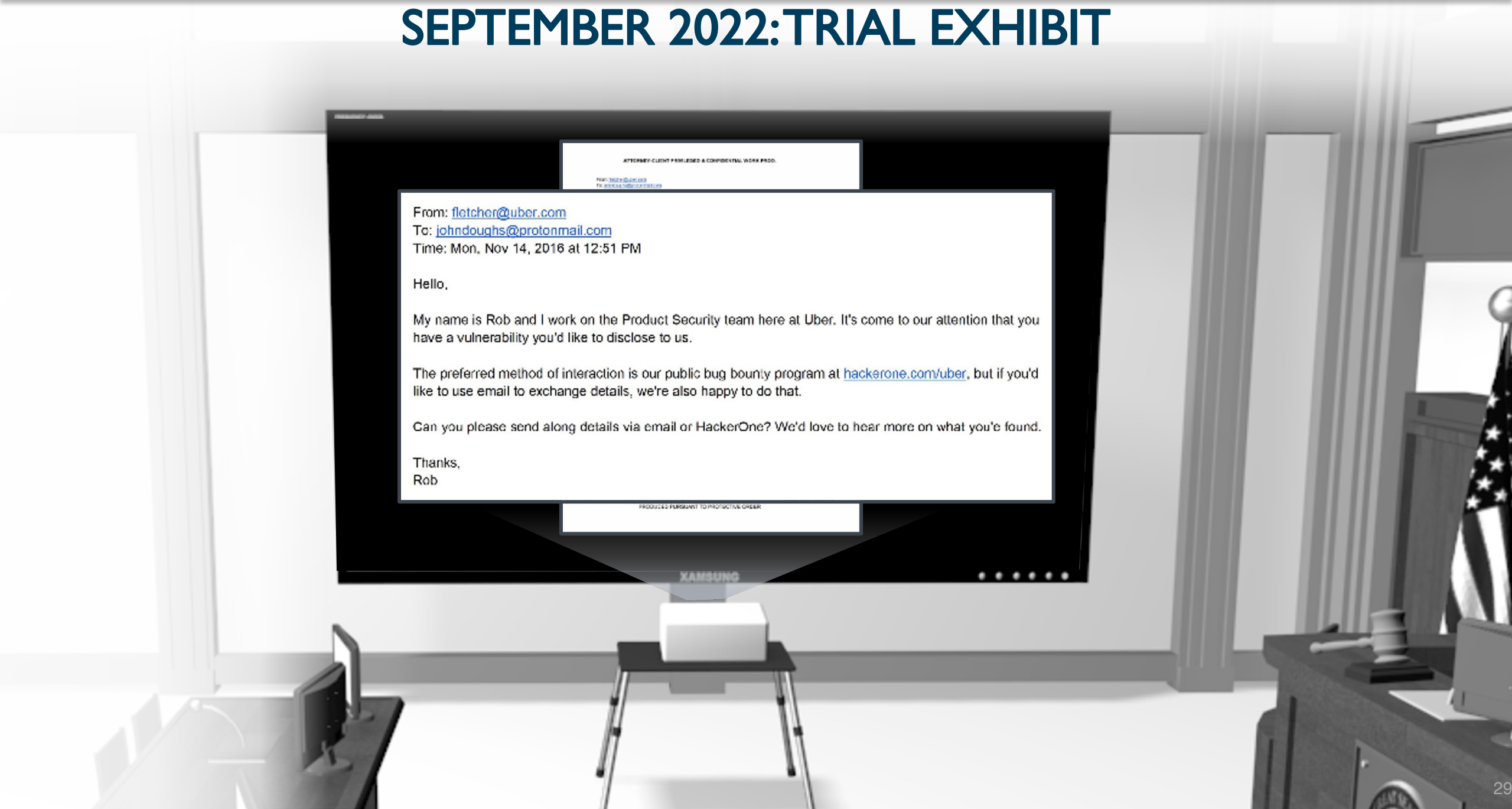
I have found a major vulnerability in uber, I was able to dump uber database and many other things.

Sent with ProtonMail Secure Email.

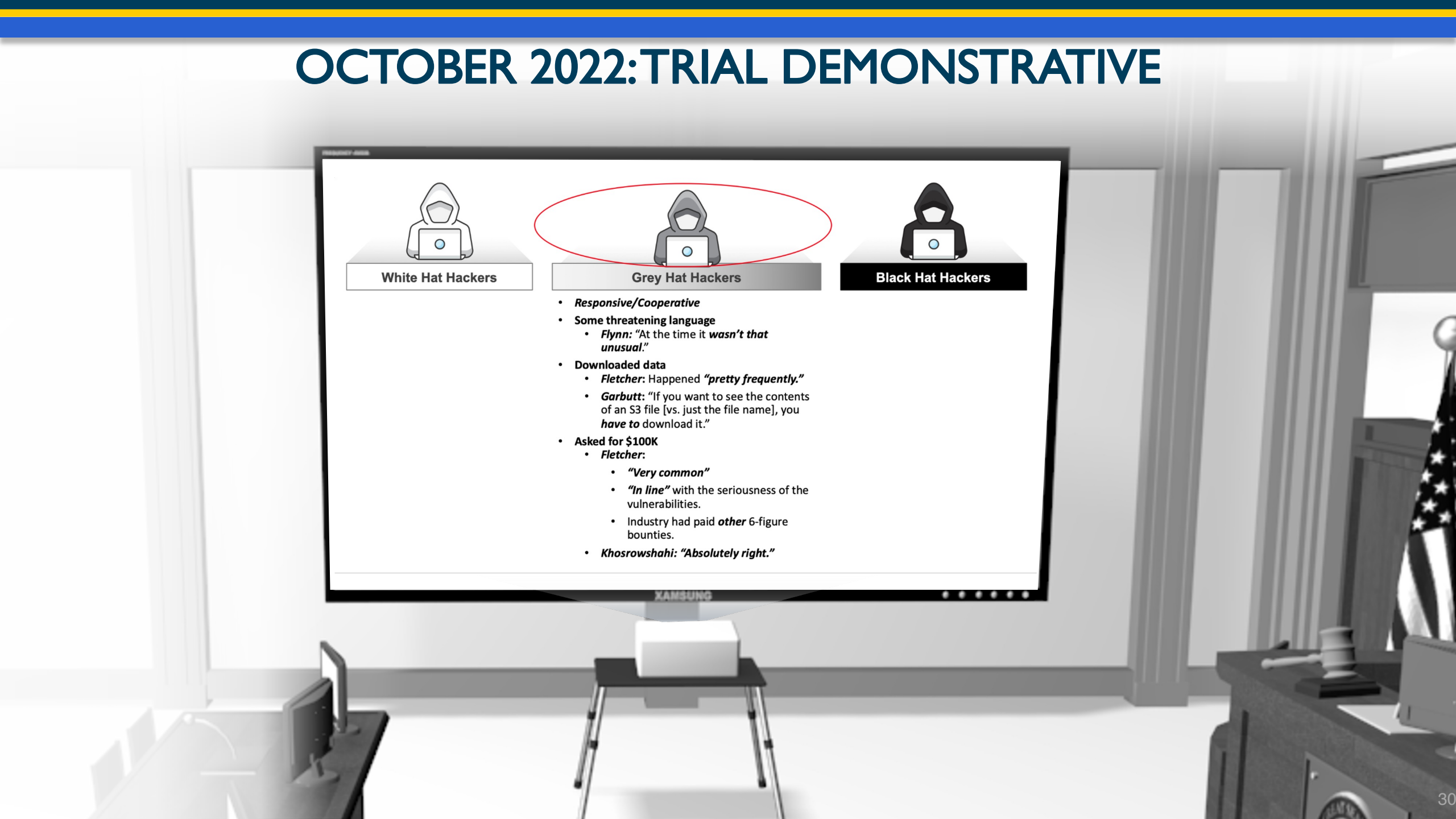
Sept 2022 | Oct 2022 | May 2023 | June 2023



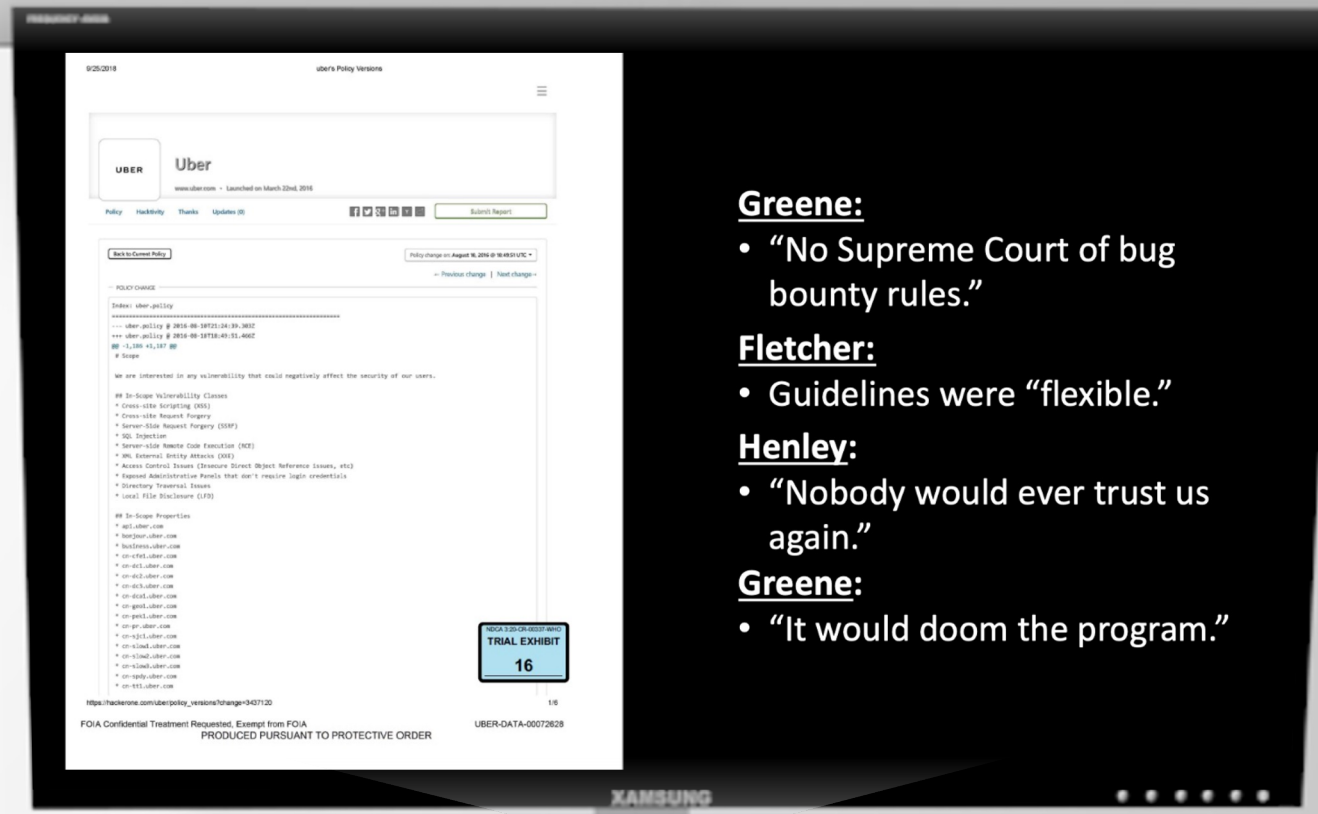
SEPTEMBER 2022: TRIAL EXHIBIT



OCTOBER 2022: TRIAL DEMONSTRATIVE



OCTOBER 2022: TRIAL DEMONSTRATIVE



Greene:

- "No Supreme Court of bug bounty rules."

Fletcher:

- Guidelines were "flexible."

Henley:

- "Nobody would ever trust us again."

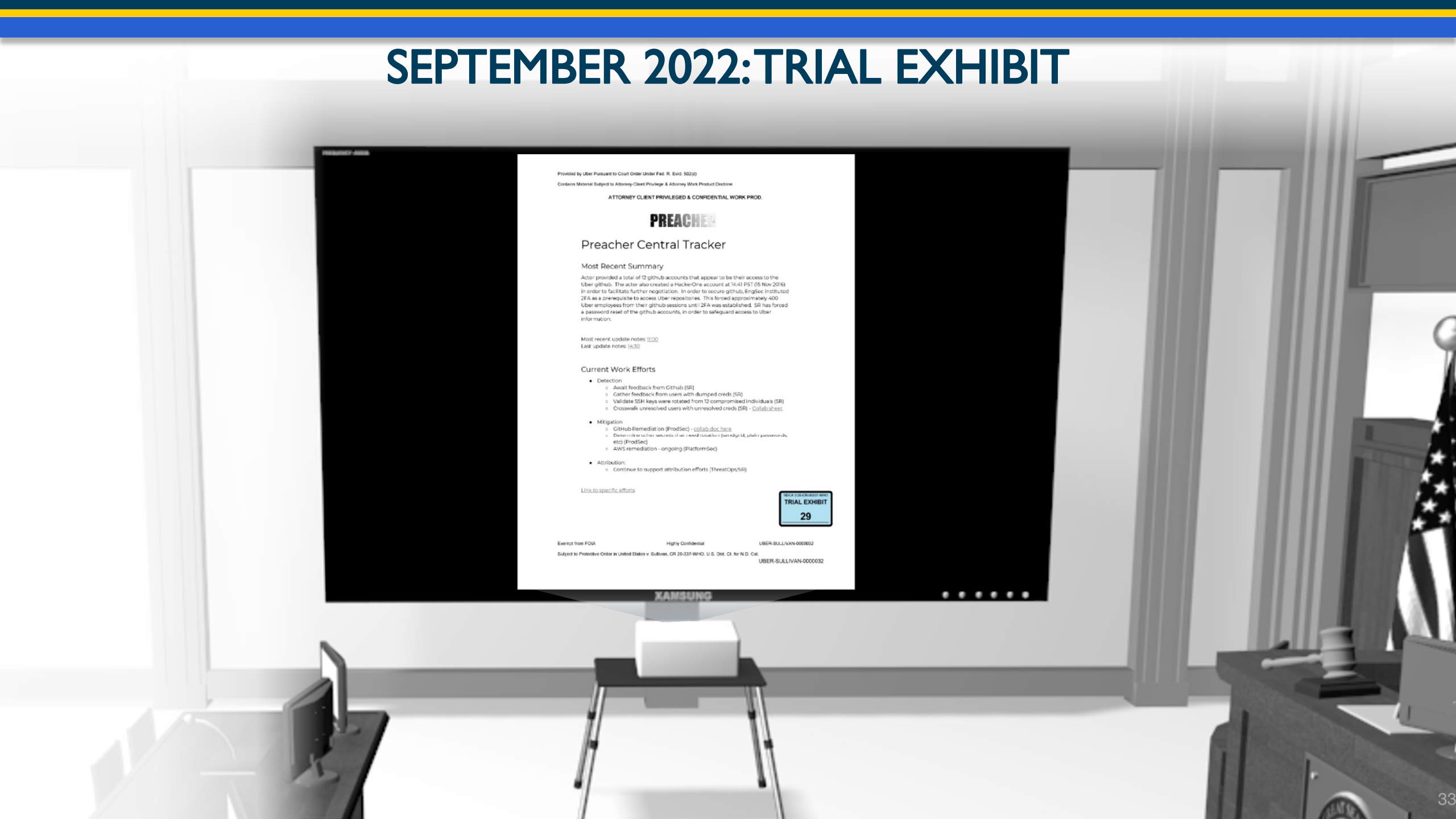
Greene:

- "It would doom the program."

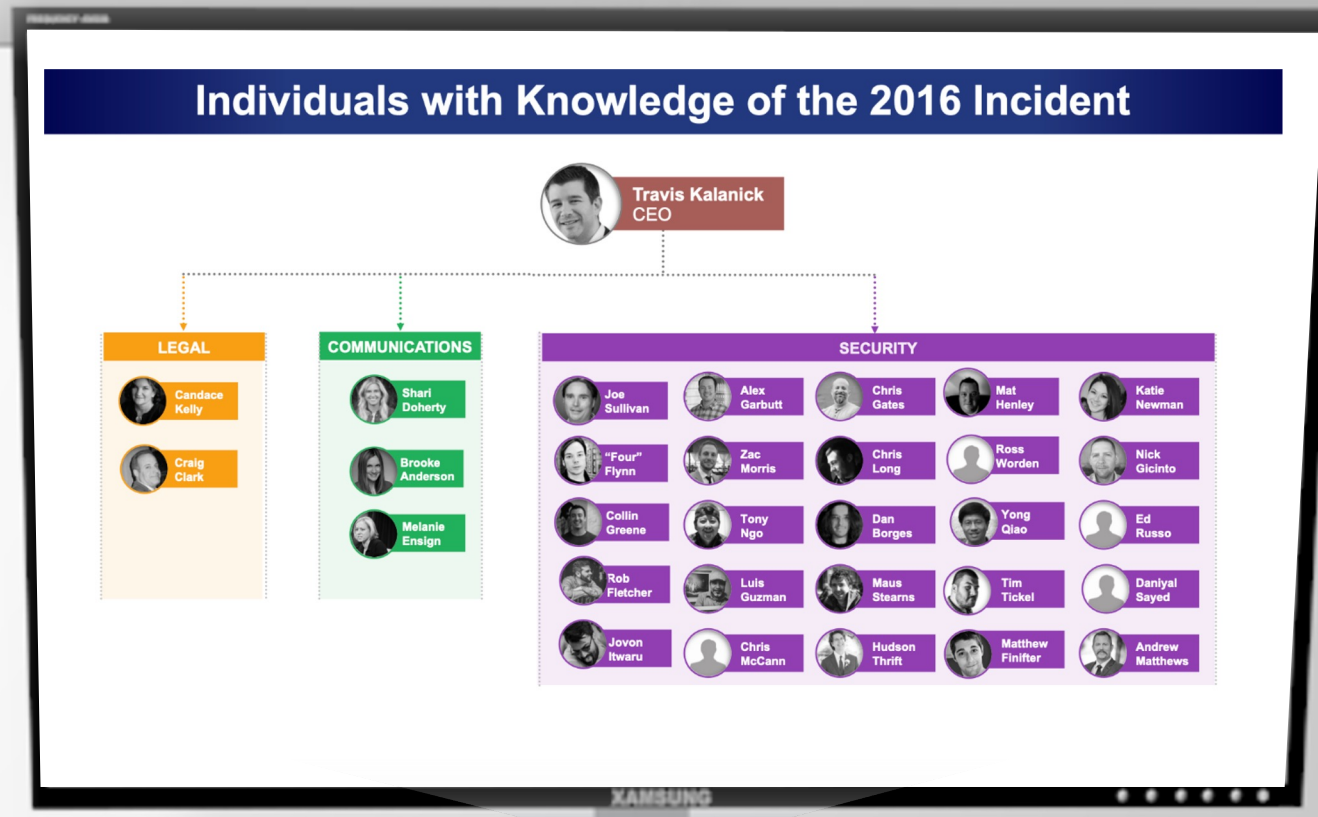
OCTOBER 2022: TRIAL DEMONSTRATIVE



SEPTEMBER 2022: TRIAL EXHIBIT



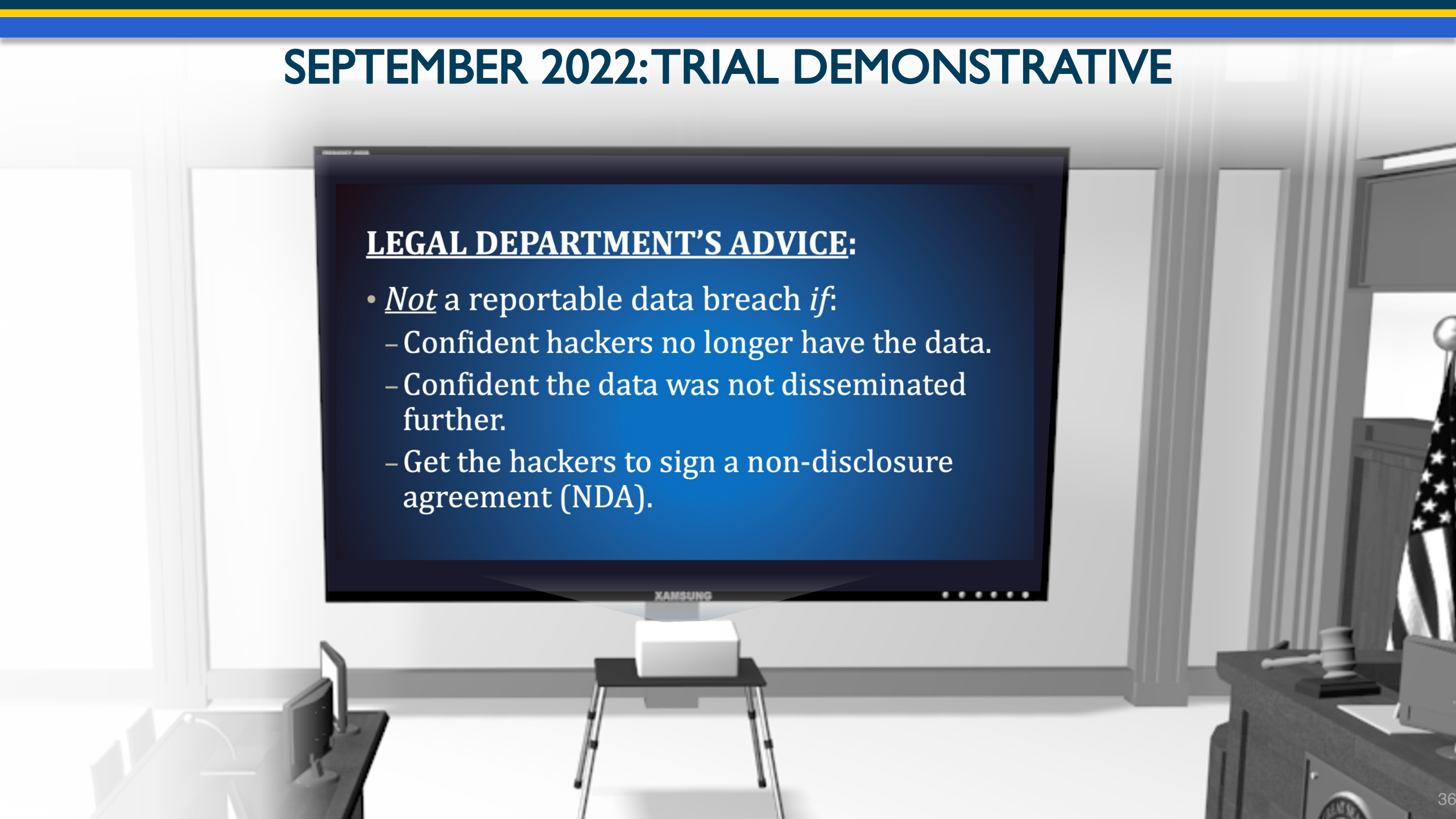
SEPTEMBER 2022: TRIAL DEMONSTRATIVE



SEPTEMBER 2022: TRIAL DEMONSTRATIVE



SEPTEMBER 2022: TRIAL DEMONSTRATIVE



Sept 2022 Oct 2022 **May 2023**

UNITED STATES OF AMERICA,	)	CR-20-00337 WHO
	)	
PLAINTIFF,	)	SAN FRANCISCO, CALIFORNIA
	)	
VS.	)	MAY 4, 2023
	)	
JOSEPH SULLIVAN,	)	PAGES 1-45
	)	
DEFENDANT.	)	
	)	

TRANSCRIPT OF PROCEEDINGS
BEFORE THE HONORABLE WILLIAM H. ORRICK
UNITED STATES DISTRICT JUDGE

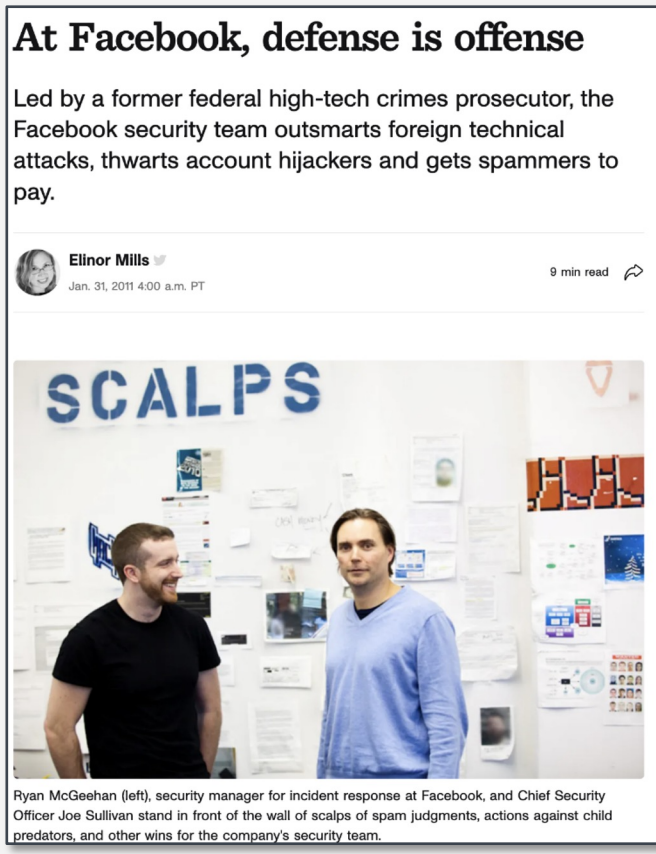
THE COURT: I'M JUST GOING AFTER THE NDA -- THE NDA ARGUMENT THAT THE GOVERNMENT MAKES, I THINK, DOESN'T REALLY FLY. THAT WASN'T AN ACT OF A COVERUP. THAT WAS PART OF THE ABILITY TO SOLVE THE PROBLEM, IN MY VIEW, IN THE WAY THAT THE EVIDENCE CAME IN.

A MOMENTARY DETOUR: ATTRIBUTION

New York Times 06/27/2020

At Facebook, defense is offense

Led by a former federal high-tech crimes prosecutor, the Facebook security team outsmarts foreign technical attacks, thwarts account hijackers and gets spammers to pay.



Ryan McGeehan (left), security manager for incident response at Facebook, and Chief Security Officer Joe Sullivan stand in front of the wall of scalps of spam judgments, actions against child predators, and other wins for the company's security team.

Joe Sullivan, the chief information security officer at the internet company Cloudflare, still remembers the frantic call he received from a colleague while working as a security executive at Facebook several years ago.

She had met a man on Match.com who claimed to work in construction in San Jose, Calif., and he had convinced her to send him a topless photo. He was threatening to email the photo to the entire company if she did not pay him $10,000.

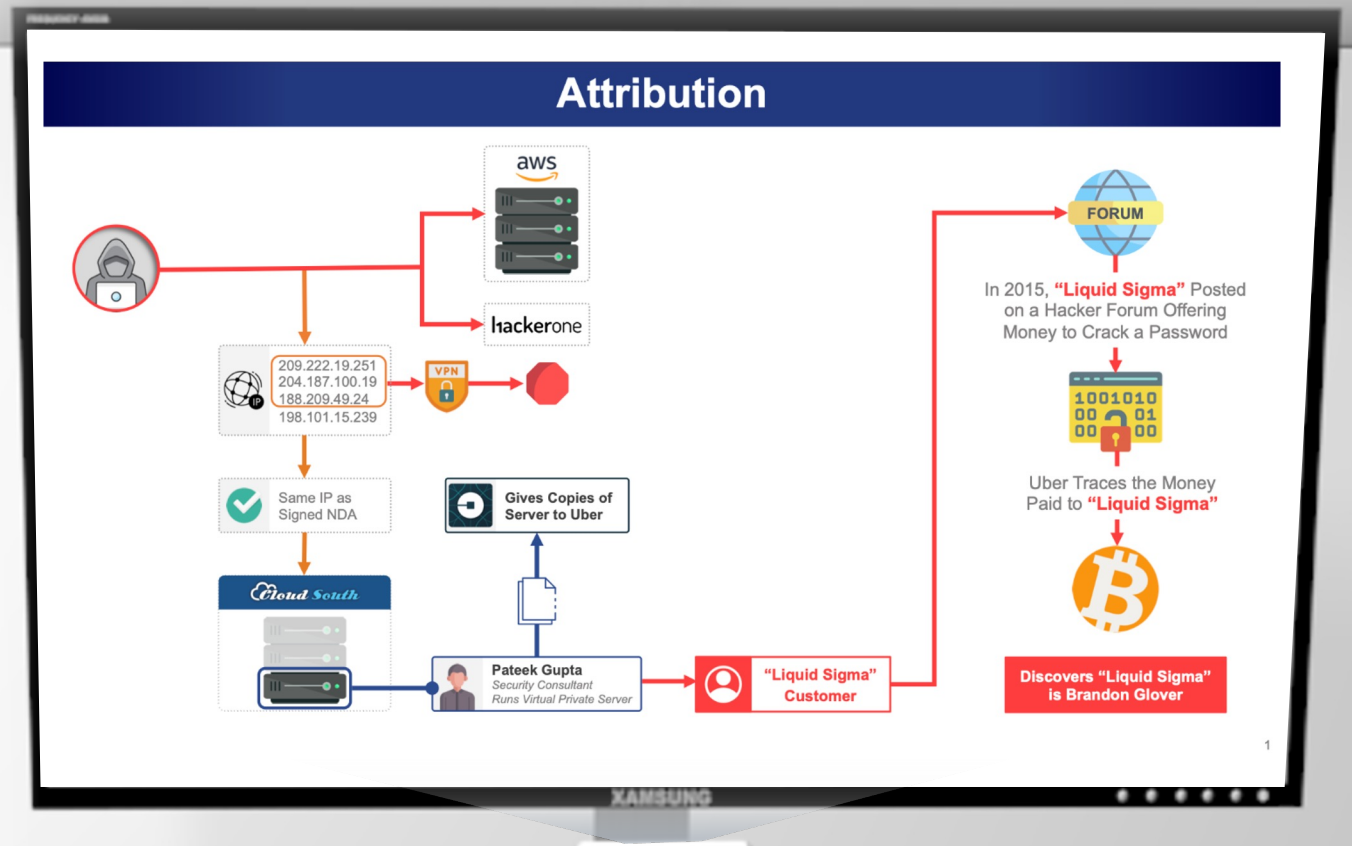
With her permission, Mr. Sullivan's team took over her account and redirected her extortionist to a payment scheme that they knew would reveal his identity. They determined he was a former Google intern living in Nigeria.

Mr. Sullivan's team hired Nigerian contractors to confront him. He confessed and surrendered access to his computer and online accounts, which showed he was extorting female executives across Silicon Valley. Investigators were able to destroy the nude photos and warned his victims not to pay.

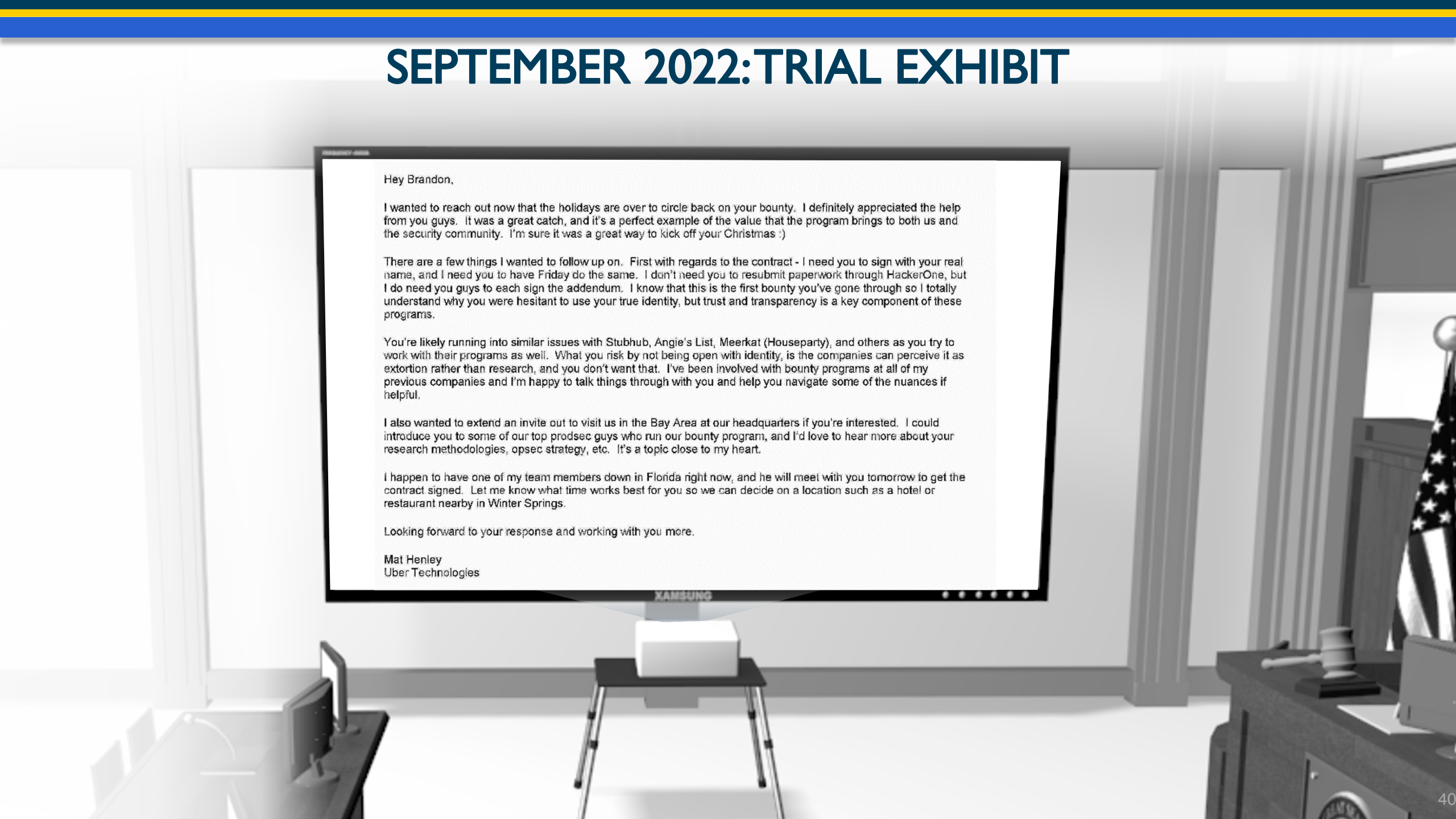
It could have taken years, Mr. Sullivan said, for law enforcement to identify the extortionist and even longer for Nigerian authorities to do something about it.

Mr. Sullivan learned that lesson as a security executive at eBay in 2006. Romanian fraudsters were running rampant on eBay, and Romanian authorities refused to address the problem. It was only after Mr. Sullivan's team shut off eBay access to all of Romania — with a message blaming eBay's shuttering on Romanian law enforcement's refusal to pursue online criminals — that Romanian police took action.

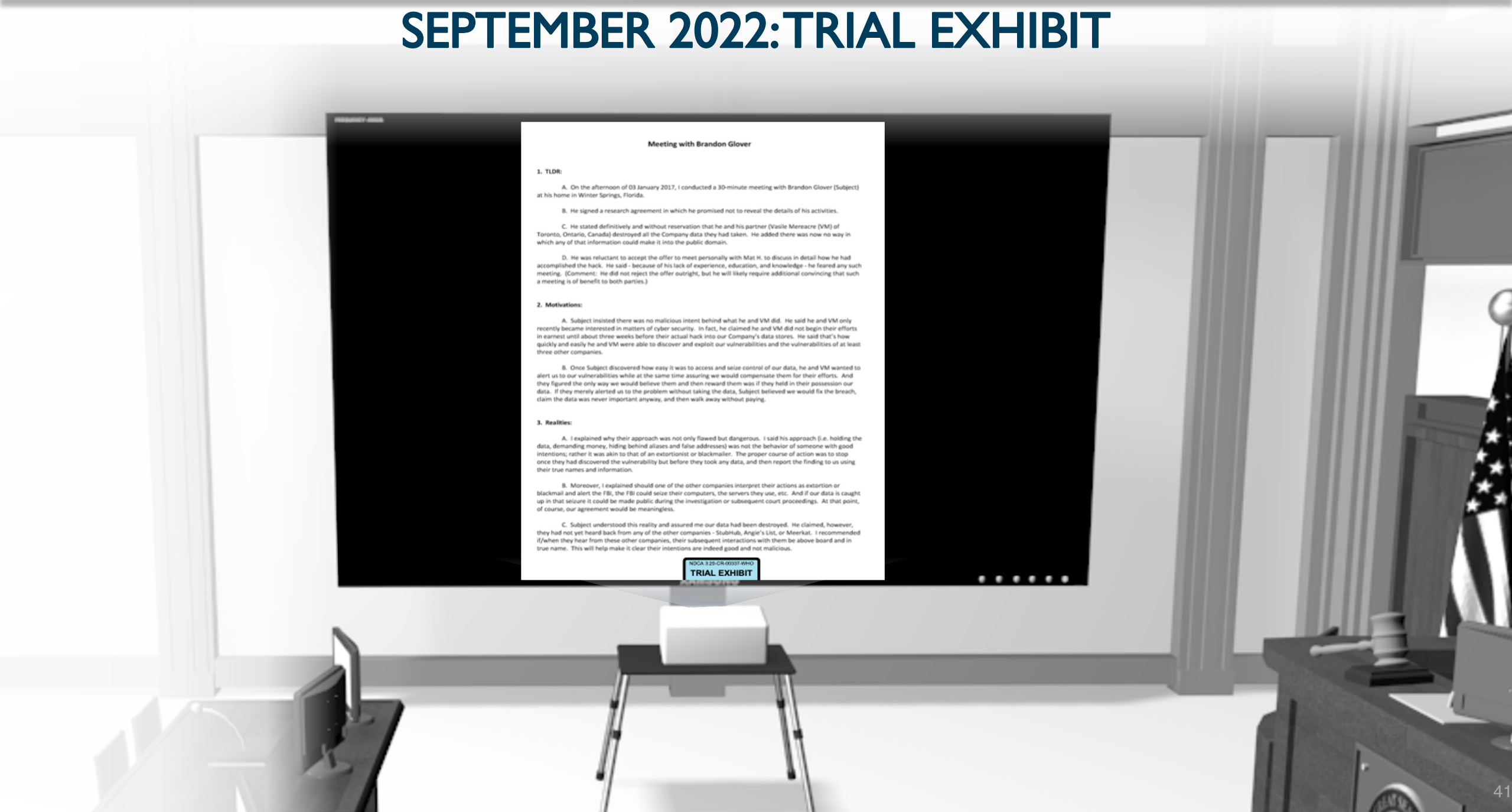
OCTOBER 2022: TRIAL DEMONSTRATIVE



SEPTEMBER 2022: TRIAL EXHIBIT



SEPTEMBER 2022: TRIAL EXHIBIT



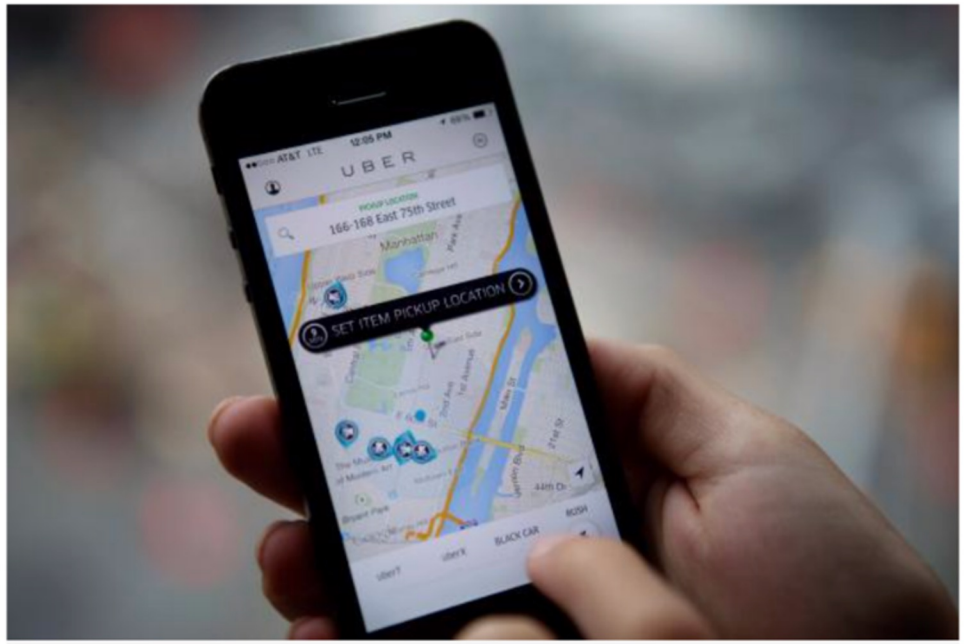
News

Newsweek

U.S.

UBER PAID 20-YEAR-OLD HACKER WHO LIVES WITH HIS MOM TO COVER UP MASSIVE DATA BREACH

BY SUMMER MEZA ON 12/7/17 AT 11:14 AM



Uber kept its largest-ever data breach secret for more than a year.
VICTOR J. BLUE/BLOOMBERG VIA GETTY IMAGES

OR

The New York Times

Inside Uber's $100,000 Payment to a Hacker, and the Fallout

Give this article



By Nicole Perlroth and Mike Isaac
Jan. 12, 2018

SAN FRANCISCO — "Hello Joe," read the November 2016 email from someone identifying himself as "John Doughs." "I have found a major vulnerability in Uber."

JURY INSTRUCTION

The elements of obtaining information from a protected computer in violation of Section 1030(a)(2)(C) of title 18 of the United States Code are:

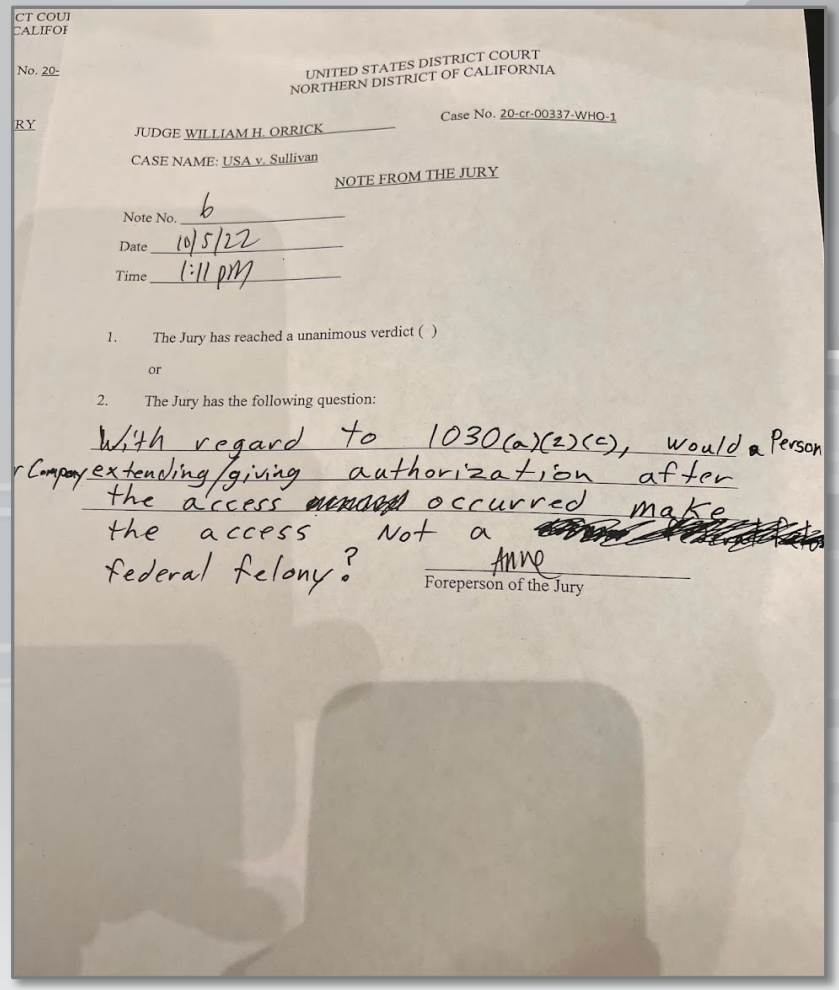
First, one or more persons intentionally accessed a computer without authorization;

Second, by accessing a computer without authorization, this person or persons obtained information from a computer that was used in or affecting interstate or foreign commerce or communications; and

Third, the value of the information obtained exceeded $5,000

Sept 2022 **Oct 2022**

NOTES FROM THE JURY DURING TRIAL



UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JUDGE WILLIAM H. ORRICK Case No. 20-cr-00337-WHO-1

CASE NAME: USA v. Sullivan

NOTE FROM THE JURY

Note No. 6
Date 10/5/22
Time 1:11 pm

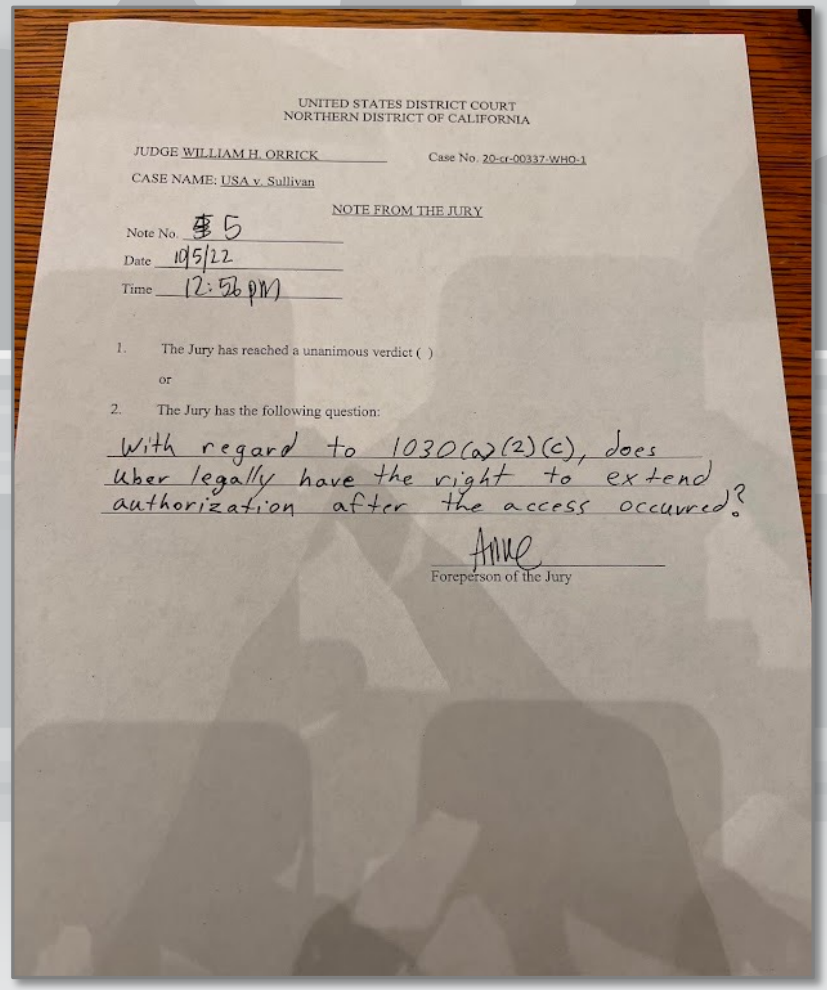
1. The Jury has reached a unanimous verdict ( )

or

2. The Jury has the following question:

With regard to 1030(a)(2)(c), would a Person or Company extending/giving authorization after the access occurred make the access Not a federal felony?

Anne
Foreperson of the Jury



UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

JUDGE WILLIAM H. ORRICK Case No. 20-cr-00337-WHO-1

CASE NAME: USA v. Sullivan

NOTE FROM THE JURY

Note No. #5
Date 10/5/22
Time 12:56 pm

1. The Jury has reached a unanimous verdict ( )

or

2. The Jury has the following question:

With regard to 1030(a)(2)(c), does Uber legally have the right to extend authorization after the access occurred?

Anne
Foreperson of the Jury

UNITED STATES DISTRICT COURT
Northern District of California

UNITED STATES OF AMERICA
v.
Brandon Charles Glover

JUDGMENT IN A CRIMINAL CASE

USDC Case Number: CR-18-00348-001 BLF
BOP Case Number: DCAN518CR00348-001
USM Number: 71232-018
Defendant's Attorney: Carleen R. Arlidge (Retained)
Albie B. Jachimowicz (Retained)

THE DEFENDANT:

☑ pleaded guilty to count: One of the Superseding Information.

☐ pleaded nolo contendere to count(s): which was accepted by the court.

☐ was found guilty on count(s): after a plea of not guilty.

The defendant is adjudicated guilty of these offenses:

Title & Section	Nature of Offense	Offense Ended	Count
18 U.S.C. §§ 1030(b) and (a)(7)(B) and (c)(3)(A)	Conspiracy to Commit Extortion Involving a Computer	January 2017	One

The defendant is sentenced as provided in pages 2 through 7 of this judgment. The sentence is imposed pursuant to the Sentencing Reform Act of 1984.

☐ The defendant has been found not guilty on count(s):

☐ Count(s) dismissed on the motion of the United States.

It is ordered that the defendant must notify the United States attorney for this district within 30 days of any change of name, residence, mailing address until all fines, restitution, costs, and special assessments imposed by this judgment are fully paid. If ordered to pay restitution, the defendant must notify the court and United States attorney of material changes in economic circumstances.

6/27/2023
Date of Imposition of Judgment

Signature of Judge
The Honorable Beth Labson Freeman
United States District Judge
Name & Title of Judge

July 7, 2023
Date

LinkedIn's Lynda.com suffers database breach

LinkedIn resets 55,000 passwords after Lynda.com experiences database breach.



Written by **Asha Barbaschow,** Contributor on Dec. 18, 2016

Online learning platform Lynda.com has begun notifying its 9.5 million users that it recently experienced unauthorised third party access to a database that contains contact information of account holders, their learning data, and courses viewed.

HENLEY - REDIRECT / FRANCIS

Q Okay. So did you contact Mr. Rou again after you figured out Brandon's true identity?

A Yes. As soon as we put our cards on the table, Mike was one of the first people I contacted to make sure they weren't in a situation.

Q And what did Mr. Rou convey to you?

A That it was a done deal. That it had passed.

A ROADMAP FOR A STRONGER PUBLIC/PRIVATE RELATIONSHIP

1. Promote more proactive communication about realities, priorities and expectations between companies/ researchers / government
2. Seek confirmation and confidence that companies can authorize security researchers' access to protect this activity (whether before or after), and that this activity won't always be considered a crime
3. Encourage more centralized CCIPS reviews before prosecutions
4. Chill out with the "just do the right thing" rhetoric from people without context on what really happened
5. Give companies the foundation to keep launching bounty programs, so it is not an exercise in accepting risk or having courage
6. Educate young people on the right ways to engage companies
7. Harmonize program policies and approaches







UKRAINE FRIENDS

www. ukrainefriends.org/donate