

To: Ramirez, Edith[eramirez@ftc.gov]
From: Edelman, R. David
Sent: Mon 10/13/2014 11:32:20 AM
Importance: Normal
Subject: Draft EO Text
MAIL_RECEIVED: Mon 10/13/2014 11:32:25 AM

Edith,

Just had a very productive discussion with both Janis and Julie – I assume the latter read it out to you. As promised, here's the

(b)(5)



R. David Edelman, Ph.D

Senior Advisor for Technology & Economic Policy

National Economic Council | OSTP | The White House

ph: (202) 456-7821 | asst: (202) 456-6010 | REdelman@ostp.eop.gov

To: Ramirez, Edith[eramirez@ftc.gov]
From: Edelman, R. David
Sent: Thur 10/9/2014 6:25:24 PM
Importance: Normal
Subject: Catching up on consumer financial protection/payment security
MAIL_RECEIVED: Thur 10/9/2014 6:25:34 PM

Hi Edith,

Hope you've been well. I wanted to get in touch, as we've finally landed what we're up to on consumer financial protection/payment security issues, and I wanted to discuss opportunities that we might find synergy with the FTC in the coming weeks. Do you have a few minutes to chat tomorrow?

All the best,

-David



R. David Edelman, Ph.D

Senior Advisor for Technology & Economic Policy

National Economic Council | OSTP | The White House

ph: (202) 456-7821 | asst: (202) 456-6010 | REdelman@ostp.eop.gov

To: Ramirez, Edith[eramirez@ftc.gov]
From: Edelman, R. David
Sent: Mon 1/12/2015 2:36:05 PM
Importance: Normal
Subject: FW: Remarks by the President at the Federal Trade Commission
MAIL_RECEIVED: Mon 1/12/2015 2:36:13 PM

Congrats on the big day!

From: White House Press Office [mailto:noreply@messages.whitehouse.gov]
Sent: Monday, January 12, 2015 1:21 PM
To: Edelman, R. David
Subject: Remarks by the President at the Federal Trade Commission

<http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd><">

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

January 12, 2015

REMARKS BY THE PRESIDENT
ON PROTECTING CONSUMERS AND FAMILIES IN THE DIGITAL AGE

Federal Trade Commission
Constitution Center
Washington, D.C.

12:15 P.M. EST

THE PRESIDENT: Thank you so much. (Applause.) Thank you. Everybody have a seat. Well, thank you, Edith, for your

introduction. Edith and I go a long way back. In law school we served on the law review together. I will not say who edited who. (Laughter.) I will say she looks exactly the same. (Laughter.) And I do not. (Laughter.) And it's upsetting. (Laughter.)

Edith, in your career, you've stood up for citizens and communities. I was proud to nominate you -- first as a commissioner, and then as chairwoman of the FTC. You are doing an outstanding job, as are your fellow commissioners, and we very much appreciate your outstanding efforts.

And Edith's story, from the daughter of Mexican immigrants to the head of the FTC, we see a central part of the American story. And that's worth remembering at a time when those are issues that we're debating all the time. It's a reminder that what makes this country special is the incredible talent that we draw from all around the world and somehow it all merges into something unique: America.

To Edith, to the fellow commissioners, to all of you who work at the FTC -- thanks for welcoming me. I'm told I may be the first President to come to the FTC in nearly 80 years, since FDR in -- (applause) -- first time apparently since FDR in 1937, which is a little surprising. I mean, you'd think like one of the Presidents would just come here by accident. (Laughter.) They ended up in the wrong building, we're already at the FTC. (Laughter.)

Anyway, I figured it was time to correct that. Plus, I know sometimes your name confuses folks. They don't always understand what your mission is. One person who does understand is David Letterman. (Laughter.) A few months ago he thanked you for standing up to the companies that were trying to pitch a new weight-loss product -- "caffeine-laced undergarments." (Laughter.) I'm actually not making this up. (Laughter.) You ruled that these products were "not substantiated by scientific evidence." (Laughter.) So, thank you for saving America from caffeine-laced undergarments. (Laughter.) These companies owed consumers a refund.

And that was just the latest example, because, as Edith said, you recently celebrated your 100th anniversary. And I want to thank you for 100 proud years of protecting American consumers. I also want to thank some of the members of Congress who are here today and many of our partners from not just government but the private sector, and consumer and privacy and advocacy groups.

Next week, just up the street, I will deliver the State of the Union address. And it will be a chance to talk about America's resurgence, including something we can all be proud of, which is the longest stretch of private sector job growth in American history -- 58 straight months and more than 11 million new jobs. (Applause.) In the speech, I'm going to focus on how we can build on that progress and help more Americans feel that resurgence in their own lives, through higher wages and rising incomes and a growing middle class.

But since I've only got two years left in this job, I tend to be impatient and I didn't want to wait for the State of the Union to start sharing my plans. So I've

been traveling across the country rolling out some of the ideas that we'll be talking about, a little bit of a sneak preview.

And in the 21st century -- in this dizzying age of technology and innovation -- so much of the prosperity that we seek, so many of the jobs that we create, so much of the opportunity that's available for the next generation depends on our digital economy. It depends on our ability to search and connect and shop and do business and create and discover and learn online, in cyberspace. And as we've all been reminded over the past year, including the hack of Sony, this extraordinary interconnection creates enormous opportunities, but also creates enormous vulnerabilities for us as a nation and for our economy, and for individual families.

So this week, I'm laying out some new proposals on how we can keep seizing the possibilities of an Information Age, while protecting the security and prosperity and values that we all cherish. Today, I'm focusing on how we can better protect American consumers from identity theft and ensure our privacy, including for our children at school. And then tomorrow, at the Department of Homeland Security, I'll focus on how we can work with the private sector to better defend ourselves against cyber-attacks. And final, on Wednesday, in Iowa, I'll talk about how we can give families and communities faster, cheaper access to broadband so they can succeed in the digital economy.

But I wanted to start here, at the FTC, because every day you take the lead in making sure that Americans, their hard-earned money and their privacy are protected, especially when they go online. And these days, that's pretty much for everything: managing our bank accounts, paying our bills, handling everything from medical records to movie tickets, controlling our homes -- smart houses, from smart phones. Secret Service does not let me do that. (Laughter.) But I know other people do.

And with these benefits come risks -- major companies get hacked; America's personal information, including financial information, gets stolen. And the problem is growing, and it costs us billions of dollars. In one survey, 9 out of 10 Americans say they feel like they've lost control of their personal information. In recent breaches, more than 100 million Americans have had their personal data compromised, like credit card information. When these cyber criminals start racking up charges on your card, it can destroy your credit rating. It can turn your life upside down. It may take you months to get your finances back in order. So this is a direct threat to the economic security of American families and we've got to stop it.

If we're going to be connected, then we need to be protected. As Americans, we shouldn't have to forfeit our basic privacy when we go online to do our business. And that's why, since I took office, we've been working with the private sector to strengthen our cyber defenses. A few months ago, we launched our BuySecure initiative. The federal government and companies across the country are moving to stronger chip-and-pin technology for credit cards. Here at the FTC, you're working with credit bureaus so that victims can recover their stolen identities faster, and every day you're helping consumers with IdentityTheft.gov

So today I'm announcing new steps to protect the identities and privacy of the American people. Let me list them for you. First, we're introducing new legislation

to create a single, strong national standard so Americans know when their information has been stolen or misused. Right now, almost every state has a different law on this, and it's confusing for consumers and it's confusing for companies -- and it's costly, too, to have to comply to this patchwork of laws. Sometimes, folks don't even find out their credit card information has been stolen until they see charges on their bill, and then it's too late. So under the new standard that we're proposing, companies would have to notify consumers of a breach within 30 days. In addition, we're proposing to close loopholes in the law so we can go after more criminals who steal and sell the identities of Americans -- even when they do it overseas.

Second, I'm pleased that more banks, credit card issuers and lenders are stepping up and equipping Americans with another weapon against identity theft, and that's access to their credit scores, free of charge. This includes JPMorgan Chase, Bank of America, USAA, State Employees' Credit Union, Ally Financial. Some of them are here today. I want to thank them for their participation. This means that a majority of American adults will have free access to their credit score, which is like an early warning system telling you that you've been hit by fraud so you can deal with it fast. And we're encouraging more companies to join this effort every day.

Third, we're going to be introducing new legislation -- a Consumer Privacy Bill of Rights. Working with many of you -- from the private sector and advocacy groups -- we've identified some basic principles to both protect personal privacy and ensure that industry can keep innovating. For example, we believe that consumers have the right to decide what personal data companies collect from them and how companies use that data, that information; the right to know that your personal information collected for one purpose can't then be misused by a company for a different purpose; the right to have your information stored securely by companies that are accountable for its use. We believe that there ought to be some basic baseline protections across industries. So we're going to be introducing this legislation by the end of next month, and I hope Congress joins us to make the Consumer Privacy Bill of Rights the law of the land.

And finally, we're taking a series of actions to protect the personal information and privacy of our children. Those of us with kids know how hard this can be. Whether they are texting or tweeting, or on Facebook, or Instagram, or Vine, our children are meeting up -- and they are growing up -- in cyberspace. It is all-pervasive. And here at the FTC, you've pushed back on companies and apps that collect information on our kids without permission.

And Michelle and I are like parents everywhere -- we want to make sure that our children are being smart and safe online. That's a responsibility of ours as parents. But we need partners. And we need a structure that ensures that information is not being gathered without us as parents or the kids knowing it. We want our kids' privacy protected -- wherever they sign in or log on, including at school.

Now, the good news is we've got new educational technologies that are transforming how our children learn. You've got innovative websites and apps and tablets, digital textbooks and tutors. Students are getting lessons tailored to their unique learning needs. We want to encourage that information. And it also facilitates teachers and parents tracking student progress and grades in real-time. And all this is part of what our ConnectedED initiative is about -- connecting 99 percent of American students to high-speed Internet so that we're empowering students, teachers, and parents, and giving them access to worlds they may never have had access to before.

But we've already seen some instances where some companies use educational technologies to collect student data for commercial purposes, like targeted advertising. And parents have a legitimate concern about those kinds of practices.

So, today, we're proposing the Student Digital Privacy Act. That's pretty straightforward. We're saying that data collected on students in the classroom should only be used for educational purposes -- to teach our children, not to market to our children. We want to prevent companies from selling student data to third parties for purposes other than education. We want to prevent any kind of profiling that outs certain students at a disadvantage as they go through school.

And we believe that this won't just give parents more peace of mind. We're confident that it will make sure the tools we use in the classroom will actually support the breakthrough research and innovations that we need to keep unlocking new educational technologies.

Now, we didn't have to completely reinvent the wheel on this proposal. Many states have proposed similar legislation. California just passed a landmark law. And I hope Congress joins us in this national movement to protect the privacy of our children.

We won't wait for legislation, though. The Department of Education is going to offer new tools to help schools and teachers work with tech companies to protect the privacy of students. As of today, 75 companies across the country have signed on to a Student Privacy Pledge. And among other things, they're committing not to sell student information or use educational technologies to engage in targeted advertising to students.

Some of those companies are here today. We want to thank you for your leadership. I want to encourage every company that provides these technologies to our schools to join this effort. It's the right thing to do. And if you don't join this effort, then we intend to make sure that those schools and those parents know you haven't joined this effort.

So, this mission, protecting our information and privacy in the Information Age, this should not be a partisan issue. This should be something that unites all of us as Americans. It's one of those new challenges in our modern society that crosses the old divides -- transcends politics, transcends ideology. Liberal, conservative, Democrat, Republican, everybody is online, and everybody understands the risks and vulnerabilities as well as opportunities that are presented by this new world.

Business leaders want their privacy and their children's privacy protected, just like everybody else does. Consumer and privacy advocates also want to make sure that

America keeps leading the world in technology and innovation and apps. So there are some basic, common-sense, pragmatic steps that we ought to all be able to support.

And rather than being at odds, I think that much of this work actually reinforces each other. The more we do to protect consumer information and privacy, the harder it is for hackers to damage our businesses and hurt our economy. Meanwhile, the more companies strengthen their cybersecurity, the harder it is for hackers to steal consumer information and hurt American families. So we've got to all be working together in the same direction, and I'm confident if we do we'll be making progress.

We are the country that invented the Internet. And we're also the pioneers of this Information Age -- the creators, the designers, the innovators. Our children are leaving us in the dust, if you haven't noticed. (Laughter.) They're connecting and they're collaborating like never before, and imagining a future we can only dream of. When we Americans put our minds together and our shoulder to the wheel, there's nothing we can't do. So I'm confident, if we keep at this, we can deliver the prosperity and security and privacy that all Americans deserve.

We pioneered the Internet, but we also pioneered the Bill of Rights, and a sense that each of us as individuals have a sphere of privacy around us that should not be breached, whether by our government, but also by commercial interests. And since we're pioneers in both these areas, I'm confident that we can be pioneers in crafting the kind of architecture that will allow us to both grow, innovate, and preserve those values that are so precious to us as Americans.

Thank you very much. And thanks to the FTC -- (applause) -- for all the great work you do to protect the American people. Thank you. (Applause.)

END 12:31 P.M. EST

[Unsubscribe](#)

To: Edelman, R. David[Ross_D_Edelman@ostp.eop.gov]
From: Edelman, R. David
Sent: Fri 10/17/2014 10:55:08 AM
Importance: Normal
Subject: FW: FACT SHEET: Safeguarding Consumers' Financial Security
MAIL_RECEIVED: Fri 10/17/2014 10:55:24 AM

Colleagues, for your awareness – please see the below release regarding the President’s remarks this morning at the Consumer Financial Protection Bureau (CFPB), announcing the new BuySecure Initiative to safeguard consumers’ financial transactions.

You can watch his remarks live at 11:45 a.m. at <http://www.wh.gov/live>.

From: White House Press Office [mailto:noreply@messages.whitehouse.gov]
Sent: Friday, October 17, 2014 10:32 AM
To: Edelman, R. David
Subject: FACT SHEET: Safeguarding Consumers’ Financial Security

THE WHITE HOUSE

Office of the Press Secretary

FOR IMMEDIATE RELEASE

October 17, 2014

FACT SHEET: Safeguarding Consumers’ Financial Security

Today, the President is signing a new Executive Order directing the government to lead by example in securing transactions and sensitive data. The new BuySecure Initiative will provide consumers with more tools to secure their financial future by assisting victims of identity theft, improving the Government’s payment security as a customer and a provider, and accelerating the transition to stronger security technologies and the development of next-generation payment security tools.

During remarks at the Consumer Financial Protection Bureau (CFPB), the President will highlight steps by his Administration and the private sector to improve security. With over 100 million Americans falling victim to data breaches over the last year, and millions suffering from credit card fraud and identity crimes, there is a need to act — and to move our economy toward stronger, more secure technologies that better secure transactions and safeguard sensitive data.

While there is no silver bullet to guarantee data security, the President is signing an Executive Order to implement enhanced security measures, including securing credit, debit, and other payment cards with microchips in lieu of basic magnetic strips, and PINs, such as those standard on consumer ATM cards. He is calling on all stakeholders to join the Administration and a number of major corporations in driving the economy toward more secure standards to safeguard consumer finances and reduce their chances of becoming victims of identity theft —

America's fastest-growing crime.

Finally today, the President will announce the White House Summit on Cybersecurity and Consumer Protection later this year to promote partnership and innovation. The Summit will bring together major stakeholders on consumer financial protection issues to discuss how all members of our financial system can work together to further protect American consumers and their financial data, now and in the future.

The President will also renew his call to Congress to enact overdue cybersecurity legislation that will help protect Americans — particularly by clarifying companies' obligations when sensitive data is breached.

KEY ACTIONS ANNOUNCED TODAY

• Moving to more secure payment systems:

As part of the President's BuySecure Initiative, he is issuing a new Executive Order that — combined with new efforts from the private sector — will help the drive the market towards more secure payment systems.

- **Making Federal payments more secure to help drive the market forward:** The President's Executive Order (EO) lays out a new policy to secure payments to and from the Federal government by applying chip and PIN technology to newly issued and existing government credit cards, as well as debit cards like Direct Express, and upgrading retail payment card terminals at Federal agency facilities to accept chip and PIN-enabled cards.

- **Companies join national effort to improve transaction security:** Home Depot, Target, Walgreens, and Walmart will be rolling out secure chip and PIN-compatible card terminals in all their stores — most by January 2015. Also in January, American Express will start a new program to support small businesses upgrading their point of sale terminals to more secure standards. Finally, Visa will launch a new program to educate consumers and merchants on chip and other secure technologies, sending experts to 20 cities in a national public service campaign.

• Preventing identity theft:

The President is also announcing new steps by the government to assist victims of identity theft, and commending actions by the private sector to help Americans stay on top of their financial health and security, through:

- **Victim resources:** The President's EO will support the Federal Trade

Commission in their development of a new one-stop resource for victims, at IdentityTheft.gov, to streamline the reporting and remediation process with credit bureaus.

- **Information sharing:** The President's EO further directs expanded information sharing, ensuring Federal investigators' ability to regularly report evidence of stolen financial and other information to companies whose customers are directly affected.
- **Company assistance:** MasterCard will also be providing its customers with free identity theft monitoring and resolution support.

● Supporting credit score transparency:

Helping consumers catch one of the best early indicators of identity theft, Citi, in partnership with FICO, will begin making credit scores available for free to all its consumer card customers updated monthly online — joining the over 70 million Americans who already have access to this feature at other nationwide banks and card issuers.

● The White House Announces the Cybersecurity and Consumer Protection Summit:

Later this year, the White House will host, in collaboration with the President's Cabinet, a summit bringing together key stakeholders in the consumer financial space to share best practices, promote adherence to stronger security standards, and discuss next generation technologies.

Leading by Example: Securing Payments Across the Economy

Federal Efforts to Transition to More Secure Payment Systems: Today, the Federal Government is making an enterprise-wide transition to more secure credit, debit, and other payment cards, as well as the retail payment terminals at government locations like the passport office, VA canteens, and national parks. These new systems will, at a minimum, meet the global security standard of more secure microchips to store card numbers instead of unencrypted magnetic strips, and secure PIN functionality, like the kind featured on most ATM cards. The goal is not just to ensure the security of doing retail business with the government, but also, through this increased demand, to help drive the market towards swifter adoption of stronger security standards. Institutions like the United States Postal Service have already made this transition across tens of thousands of retail facilities across the country.

● *Making Chip and PIN Cards the Standard for the Federal Government:* These “chip and PIN” cards, which have cut down on payment fraud considerably in other countries, will become the standard for Federal Government programs like SmartPay® and Direct Express®. We are working with these programs to ensure that we begin a replacement program on January 1, 2015, and will, within the calendar year, issue over one million new, more secure government payment cards.

● *Updating to Chip and PIN Card Terminals in Federal Agencies Processing Consumer Sales:* Every Federal agency processing consumer sales will actively replace any prior-generation card retail payment card

terminals to those with new chip and PIN security features under a plan issued by Department of the Treasury, which establishes requirements that federal agencies must follow when receiving credit and debit card payments when using Treasury's collection system.

Building Public-Private Awareness About More Secure Authentication: In the next eighteen months, government agencies will ensure personal data digitally released by the government to citizens goes through multiple tests for authentication so that every citizen's personal information is protected by the most secure methods possible, consistent with a plan the National Security Council Staff, Office of Science and Technology Policy, and Office of Management and Budget will present to the President.

Helping Americans Secure Their Good Name: Improving Resources to Identify and Remediate Identity Theft:

Today, the President is also announcing new steps by the government to assist victims of identity theft, and commending actions by the private sector to help Americans stay on top of their financial health and security, through:

- **Credit Score Transparency.** Under the leadership of the Consumer Financial Protection Bureau, a number of leaders in the financial services industry will be making credit scores more readily available to all Americans — improving consumers' awareness of credit health, and helping them identify major shifts in their credit score, a key first sign of identity theft.
 - Beginning in January **Citi**, in partnership with **FICO**, will be making free credit scores available online to consumers with Citi branded credit cards —this score will be updated monthly and is the same score Citi Cards uses in lending decisions.
 - This announcement builds on work done by institutions like Discover, Barclaycard, Pentagon Federal Credit Union, and First National Bank of Omaha who, since implementing similar systems, have provided over 70 million Americans with access to their scores to track their credit health.

- **Improving Identity Theft Resources.** The Department of Justice, Department of Commerce, and Social Security Administration are also working to make the fraud reporting process as easy as possible for Americans who have experienced credit card fraud. Their goal is to, within two years, reduce by half the amount of time it takes consumers to remediate the average case of identity theft. To do that, they will:
 - Streamline all necessary sources of information so that visitors to IdentityTheft.gov will be equipped with the resources they need to combat fraud, all in one place, and can more quickly resolve and remediate incidents of identity theft.
 - Build upon the IdentityTheft.gov platform, in partnership with credit bureaus, to develop a more user-friendly and accessible portal that helps digitally submit reports of fraud to multiple credit bureaus.

- **Company Assistance.** Before year's end, **MasterCard** will offer all its credit, debit, prepaid and small business card holders free, 24/7 identity theft resolution support and online identity monitoring services.

Enhanced Information Sharing: Finally, to enhance companies' and consumers' ability to respond quickly to incidents of fraud, as they occur, the Department of Justice and Federal Bureau of Investigation will improve and

coordinate efforts to regularly submit information about compromised accounts and other information to the National Cyber-Forensics and Training Alliance's Internet Fraud Alert System.

Private Sector Action to Transition to More Secure Payment Technologies: The President has also called on industry to ensure that consumers know the security of their information is being taken seriously, and to empower citizens with more tools to help safeguard the data that matters most. Some of the nation's largest retailers, card issuers, payment networks, and banks are coming together to secure their own systems, and offer more secure options for their customers. That's why today, the President is commending private sector steps taken in that direction, including:

- **American Express:** In January 2015, American Express will launch a \$10 million program to assist small business customers in upgrading their point of sale terminals.
- **Home Depot:** In addition to transitioning 85,000 point of sale terminals to support chip and PIN in stores, Home Depot has completed a major new payment security project that provides enhanced encryption of payment data at point of sale in the company's U.S. stores.
- **Target:** As of this month, Target has completed installation of chip and PIN readers in all its 1,801 stores. Starting in early 2015, stores will begin accepting all chip-enabled cards and reissuing more than 20 million Target-brand chip and PIN enabled credit and debit cards.
- **Visa:** Visa will invest more than \$20 million to educate consumers and merchants on chip and other secure technologies, while also sending experts to 20 cities in a national public service campaign.
- **Walgreens:** As of today, Walgreens has chip and PIN readers in all its 8,200 stores, and starting in early 2015, stores will begin accepting cards with these upgraded features.
- **Walmart:** By November 1, 2014, all of the nearly 5,000 Walmart and Sam's Club U.S. stores will have activated chip and PIN readers.

The Continued Need for Congress to Act on Data Breach and Cybersecurity Legislation: While President Obama and his Administration continue to take every possible step to secure our transactions and information, it remains clear that American businesses and consumers demand Congressional action.

As the President outlined in his Cybersecurity Legislative Proposal and as was reiterated in the recent report to the President on Big Data, the current patchwork of laws governing a company's obligations in the event of a data breach is unsustainable, and helps no one.

- *Data Breach Legislation:* Today we are calling on Congress to act with urgency on data breach legislation, to bring clarity to the expectations consumers should have when their data has been breached, and to steps companies must take to notify their customers of risks after such security breaches.
- *Cybersecurity Legislation:* We are also calling on Congress to pass meaningful cybersecurity legislation that will help the Government better protect Federal networks and legislation that appropriately balances the need for greater information sharing and strong protection for privacy and civil liberties — respecting the longstanding responsibilities of civilian and military agencies.

###

To: Ramirez, Edith[eramirez@ftc.gov]
From: Edelman, R. David
Sent: Mon 1/12/2015 9:13:52 AM
Importance: Normal
Subject: FW: FACT SHEET: Safeguarding American Consumers & Families
MAIL_RECEIVED: Mon 1/12/2015 9:13:57 AM

-----Original Message-----

From: White House Press Office [noreply@messages.whitehouse.gov]
Sent: Monday, January 12, 2015 06:10 AM Eastern Standard Time
To: Edelman, R. David
Subject: FACT SHEET: Safeguarding American Consumers & Families

THE WHITE HOUSE

Office of the Press Secretary

FOR IMMEDIATE RELEASE

January 12, 2015

**FACT SHEET: Safeguarding American Consumers & Families
President Obama Announces New Privacy Protections for the Digital Age**

Today, President Obama will build on the steps he has taken to protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties. These actions have included the President's 2012 comprehensive blueprint for consumer privacy, the BuySecure initiative—launched last year—to safeguard Americans' financial security, and steps the President took earlier this year by creating a working group of senior administration officials to examine issues related to big data and privacy in public services and the commercial sector.

In an increasingly interconnected world, American companies are also leaders in protecting privacy, taking unprecedented steps to invest in cybersecurity and provide customers with precise control over the privacy of their online content. But as cybersecurity threats and identity theft continue to rise, recent polls show that 9 in 10 Americans feel they have in some way lost control of their personal information — and that can lead to less interaction with technology, less innovation, and a less productive economy.

At the Federal Trade Commission offices today, President Obama will highlight measures he will discuss in the State of the Union and unveil the next steps in his comprehensive approach to enhancing consumers' security, tackling identity theft, and improving privacy online and in the classroom. These steps include:

Improving Consumer Confidence by Tackling Identity Theft

• **□□□□□□□ The Personal Data Notification & Protection Act:** The President is putting forward a new legislative proposal to help bring peace of mind to the tens of millions of Americans whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been exposed, including establishing a 30-day notification

requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The proposal also criminalizes illicit overseas trade in identities.

- **Identifying and Preventing Identity Theft:** To give consumers access to one of the best early indicators of identity theft, as well as an opportunity to improve their credit health, JPMorganChase and Bank of America, in partnership with Fair Isaac Corporation (FICO), will join the growing list of firms making credit scores available for free to their consumer card customers. USAA and State Employees' Credit Union will also offer free credit scores to their members, and Ally Financial is further widening the community of companies taking this step by making credit scores available to their auto loan customers. Through this effort over half of all adult Americans with credit scores will now have access to this tool to help spot identity theft, through their banks, card issuers, or lenders.

Safeguarding Student Data in the Classroom and Beyond

-

- **The Student Digital Privacy Act:** The President is releasing a new legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technology — by ensuring that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute, builds on the recommendations of the White House Big Data and Privacy review released earlier this year, would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school — while still permitting important research initiatives to improve student learning outcomes, and efforts by companies to continuously improve the effectiveness of their learning technology products.

- **New Commitments from the Private Sector to Help Enhance Privacy for Students:** Today 75 companies have committed to the cause, signing a pledge to provide parents, teachers, and kids themselves with important protections against misuse of their data. This pledge was led by the Future of Privacy Forum and the Software & Information Industry Association, and today the President challenged other companies to follow their lead.

- **New Tools from the Department of Education to Empower Educators Around the Country and Protect Students:** The Department of Education and its Privacy Technical Assurance Center play a critical role in protecting American children from invasions of privacy. Today, we are announcing a forthcoming model terms of service, as well as teacher training assistance that will enhance our ability to help ensure educational data is used appropriately and in accordance with the educational mission.

Convening the Public and Private Sector to Tackle Emerging Privacy Issues

- **Voluntary Code of Conduct for Smart Grid Customer Data Privacy:** Today the Department of Energy and the Federal Smart Grid Task Force are releasing a new Voluntary Code of Conduct (VCC) for utilities and third parties aimed at protecting electricity customer data — including energy usage information. This Code reflects a year of expert and public consultation, including input from industry stakeholders, privacy experts, and the public. As companies begin to sign on, the VCC will help improve consumer awareness, choice and consent, and controls on access.

-

Promoting Innovation by Improving Consumers Confidence Online

- **Consumer Privacy Bill of Rights Legislation:** Online interactions should be governed by clear principles — principles that look at the context in which data is collected and ensure that users' expectations are not abused. Those were the key themes of the Administration's 2012 *Consumer Privacy Bill of Rights*, and today the Commerce Department announced it has completed its public consultation on revised draft legislation

enshrining those principles into law. Within 45 days, the Administration will release this revised legislative proposal and today we call on Congress to begin active consideration of this important issue.

-

These actions build on steps the President has already taken to support consumer privacy and fight identity theft, including:

• **██████████ Making Federal Payments More Secure to Help Drive the Market Forward:** In October, as part of his BuySecure Initiative, the President issued an Executive Order laying out a new policy to secure payments to and from the Federal government by applying chip and PIN technology to newly issued and existing government credit cards, as well as debit cards like Direct Express, and upgrading retail payment card terminals at Federal agency facilities to accept chip and PIN-enabled cards. This accompanied an effort by major companies like Home Depot, Target, Walgreens, and Walmart to roll out secure chip and PIN-compatible card terminals in stores across the country.

• **██████████ New Measures to Prevent Identity Theft:** The President also announced new steps by the government to assist victims of identity theft, including supporting the Federal Trade Commission in their development of a new one-stop resource for victims at IdentityTheft.gov and expanding information sharing to ensure Federal investigators' ability to regularly report evidence of stolen financial and other information to companies whose customers are directly affected.

###

[Unsubscribe](#)

To: Ramirez, Edith[eramirez@ftc.gov]
From: Ted Dean
Sent: Wed 10/29/2014 1:20:04 PM
Importance: Normal
Subject: FW: Letter on behalf of Mr Paul Nemitz to your attention
MAIL_RECEIVED: Wed 10/29/2014 1:20:12 PM
[letter to Ted Dean.pdf](#)

Hi Edith,

Following up on our conversation (b)(5) Do you have a few minutes for a quick call?

(b)(5) Please see attached.

Regards,

Ted

Non Responsive

Non Responsive

Duplicate

Duplicate

To: Ramirez, Edith[eramirez@ftc.gov]
From: Baer, Bill
Sent: Thur 12/11/2014 8:18:05 PM
Importance: Normal
Subject: hi
MAIL_RECEIVED: Thur 12/11/2014 8:18:08 PM

congrats on the New England Journal piece. absolutely terrific.

(b)(5)

OK?

Bill

Non Responsive

From: Ted Dean [<mailto:Ted.Dean@trade.gov>]
Sent: Monday, October 20, 2014 8:24 AM
To: Ramirez, Edith
Subject: safe harbor

Hi Edith,

Great to see you in Mauritius. Hope you are recovered from the flight back. (Our stay was a bit shorter than the FTC's but I calculated we were traveling for close to 60 hours of a 144 hour trip...)

I wanted to follow-up on our conversation on Safe Harbor. The report I mentioned that was released by the Office of the Director of National Intelligence is available at: <http://www.dni.gov/index.php/newsroom/reports-and-publications/204-reports-publications-2014/1126-interim-progress-report-on-implementing-ppd-28>.

I need a day or two to coordinate with some folks here about next steps, but perhaps we could aim to speak towards the middle or end of the week. Please let me know how your schedule looks wed to fri.

Thanks,

Ted

To: Ramirez, Edith[eramirez@ftc.gov]
Cc: Kestenbaum, Janis[jkestenbaum@ftc.gov]
From: Edelman, R. David
Sent: Mon 10/13/2014 12:05:52 PM
Importance: Normal
Subject: RE: Draft EO Text
MAIL_RECEIVED: Mon 10/13/2014 12:05:55 PM

Thanks, Edith, and appreciate you spending time on this from afar.

(b)(5)

Looking forward to hearing from Janis tomorrow -- and of course, both Jeff and I are happy to get on the phone with you all to talk through.

All the best,

-rD

From: Ramirez, Edith [mailto:eramirez@ftc.gov]
Sent: Monday, October 13, 2014 12:01 PM
To: Edelman, R. David
Cc: Kestenbaum, Janis
Subject: Re: Draft EO Text

David,

(b)(5)

Edith

From: Edelman, R. David [mailto:Ross_D_Edelman@ostp.eop.gov]
Sent: Monday, October 13, 2014 11:32 AM
To: Ramirez, Edith
Subject: Draft EO Text

Edith,

(b)(5)



R. David Edelman, Ph.D

Senior Advisor for Technology & Economic Policy

National Economic Council | OSTP | The White House

ph: (202) 456-7821 | asst: (202) 456-6010 | REdelman@ostp.eop.gov

Non Responsive

> On Dec 11, 2014, at 7:29 PM, Ramirez, Edith <eramirez@ftc.gov> wrote:

> (b)(5)

> -----Original Message-----

> From: Baer, Bill [mailto:Bill.Baer@usdoj.gov]

> Sent: Thursday, December 11, 2014 7:18 PM

> To: Ramirez, Edith

> Subject: hi

>

> congrats on the New England Journal piece. absolutely terrific.

Duplicate

> OK?

>

> Bill

>

>

To: Ramirez, Edith[eramirez@ftc.gov]
Cc: Watson, Shaundra[SWATSON@ftc.gov]
From: Edelman, R. David
Sent: Thur 1/8/2015 9:34:34 AM
Importance: Normal
Subject: Student Privacy Draft Bill
MAIL_RECEIVED: Thur 1/8/2015 9:34:39 AM
[StudentPrivacyLaw_2015010_0845.docx](#)

Edith,

(b)(5)

Looking forward to catching up in the next few days.

All the best,

-rD



R. David Edelman

Senior Advisor for Technology & Economic Policy
direct: (202) 456-7821 | topline: (202) 456-6010

Duplicate

To: Ramirez, Edith[eramirez@ftc.gov]
Cc: Mielke, Dawn M.[Dawn_M._Mielke@ostp.eop.gov]; Smith, Megan[Megan_J_Smith@ostp.eop.gov]
From: Macgillivray, Alexander
Sent: Mon 1/26/2015 1:22:28 PM
Importance: Normal
Subject: Time w/ CTO Team
MAIL_RECEIVED: Mon 1/26/2015 1:22:31 PM

Chairwoman Ramirez,

It was wonderful to be your guest at the President's privacy focused event on the 12th. Thank you.

If your schedule permits, Megan and I would love to give you and your staff a brief overview of team CTO and the work we have on our agenda. Much of it is consistent with the FTC's strong direction on privacy, competition, and consumer protection work.

-Alex



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

January 26, 2015

The Honorable Lori Swanson
Attorney General of Minnesota
1400 Bremer Tower
445 Minnesota Street
St. Paul, MN 55101

Dear Attorney General Swanson:

Thank you for your December 10, 2014 letter regarding the proposed merger of US Foods, Inc. and Sysco Corporation. We appreciate receiving the information and views presented in your correspondence.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the public disclosure of the details of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction. I can assure you that, as in all our merger reviews, the Commission is committed to conducting a thorough investigation of competitive effects in all relevant markets likely to be affected by the transaction. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you for bringing your concerns to our attention in this important matter. The Commission appreciates your interest in this subject and, as always, the willingness of your office to work together with the Commission on such matters of mutual interest.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE ATTORNEY GENERAL

State of Minnesota

ST. PAUL, MN 55155

LORI SWANSON
ATTORNEY GENERAL

December 10, 2014

The Honorable Edith Ramirez, Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue Northwest
Washington, DC 20580

Re: Proposed merger of Sysco Corporation and US Foods, Inc.

Dear Chairwoman Ramirez:

I am aware that the Federal Trade Commission is currently reviewing the proposed merger between Sysco and US Foods. I write to share my concerns about the impact of this merger on competition within the food distribution industry.

As you know, Sysco and US Foods are the two largest broadline food distributors in the nation. Sysco operates approximately 151 distribution centers in the United States and reported \$46 billion in revenue during fiscal year 2014. US Foods operates approximately 77 distribution centers nationwide and reported annual revenue of \$22 billion. By contrast, the next largest competitor, Performance Food Group, reported revenue of only about \$14 billion last fiscal year. In short, a combined Sysco/US Foods would dwarf any rivals, which raises serious questions about the robustness of the competition that would remain in the industry if the merger were to occur.

The creation of such a company has implications not only for customers who benefit from the presence of competing, nationwide food distributors, but also for customers whose operations are limited to a particular region or state. Minnesota's restaurant industry includes both chains that require distribution throughout the state and many restaurants with a single location. This Office has received feedback from multiple Minnesota-based restaurants expressing concerns that the merger of Sysco and US Foods will hurt competition within the food distribution industry, leaving them with fewer choices among distributors and potentially resulting in higher prices for consumers.

Minnesota--and Minneapolis in particular--was known as the milling capital of the world at the beginning of the twentieth century. This agricultural footing continues today, as the total value of the crops and livestock Minnesota farmers produce places it among the top five agricultural states in the nation. In particular, Minnesota is one of the largest producers of grains, soybeans, and milk, as well as livestock such as turkeys and hogs. The merger has the

The Honorable Edith Ramirez, Chairwoman
Federal Trade Commission
December 10, 2014
Page 2

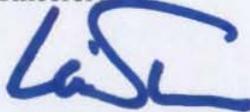
potential to affect Minnesota farmers and other producers of agricultural products purchased by the companies.

Public institutions—such as school districts, universities, and public hospitals—also frequently contract with a food distributor to handle their food service needs. They often do so by issuing requests for proposals containing particular requirements that an eligible distributor must satisfy. The presence of independent Sysco and US Foods—both of which can generally meet the requirements of any RFP given their scale, and which frequently bid against one another—helps ensure that public institutions in Minnesota (and presumably, across the country) receive the best prices and service when selecting a food distributor. A merger of these companies would significantly alter the competitive dynamics present in such RFPs.

It is questionable whether any amount of divestiture can recreate the loss of US Foods as a strong competitor in the broadline food distribution market. I encourage the Commission to closely scrutinize the proposed merger between Sysco and US Foods to ensure that it does not adversely affect competition within the food distribution industry, both in Minnesota and nationally.

I thank you for your attention to this important matter.

Sincerely



LORI SWANSON
Attorney General

cc: The Honorable Julie Brill, Commissioner
The Honorable Maureen K. Ohlhausen, Commissioner
The Honorable Joshua D. Wright, Commissioner
The Honorable Terrell McSweeney, Commissioner

Non Responsive

From: Cyber Summit [mailto:cybersummit@who.eop.gov]
Sent: Friday, February 06, 2015 12:39 PM
To: Ramirez, Edith
Subject: Invitation: White House Cybersecurity Summit on February 13



Greetings,

You are invited to attend the full-day White House Summit on Cybersecurity and Consumer Protection at Stanford University on Friday, February 13th. The Summit will feature remarks by President Obama and bring together major stakeholders on cybersecurity and consumer protection issues to help shape public and private sector efforts to protect American consumers and companies from growing threats to consumers and commercial networks. Lunch will be provided by Stanford University.

From increasing cybersecurity information sharing to improving adoption of more secure payment technologies, here's a look at the topics that panels at the Summit will address:

- Public-Private Collaboration on Cybersecurity
- Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations
- Promoting More Secure Payment Technologies
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation on Cybersecurity
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

This invitation is non-transferable. **RSVP for the Summit [here](#) by Monday, February 9th**. You will receive a confirmation e-mail with arrival and logistical instructions next week. Please expect to arrive at

the Summit before 8:00am and depart after 4:30pm.

Due to the high interest in the Summit, we ask that you only register if you are able to attend the full day-long program. If you are not able to attend the full program and would like to just attend the morning session, when we expect President Obama to speak, please e-mail cybersummit@who.eop.gov for the separate RSVP process for morning-only attendees. At this time we are not able to share the full agenda for the Summit. As more details become available they will be posted on WhiteHouse.gov/CyberSummit.

If you have any questions please e-mail cybersummit@who.eop.gov.

Sincerely,

The White House Office of Public Engagement



Non Responsive

From: Cyber Summit [mailto:cybersummit@who.eop.gov]
Sent: Friday, February 06, 2015 12:39 PM
To: Ramirez, Edith
Subject: Invitation: White House Cybersecurity Summit on February 13



Greetings,

You are invited to attend the full-day White House Summit on Cybersecurity and Consumer Protection at Stanford University on Friday, February 13th. The Summit will feature remarks by President Obama and bring together major stakeholders on cybersecurity and consumer protection issues to help shape public and private sector efforts to protect American consumers and companies from growing threats to consumers and commercial networks. Lunch will be provided by Stanford University.

From increasing cybersecurity information sharing to improving adoption of more secure payment technologies, here's a look at the topics that panels at the Summit will address:

- Public-Private Collaboration on Cybersecurity
- Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations
- Promoting More Secure Payment Technologies
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation on Cybersecurity
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

This invitation is non-transferable. **RSVP for the Summit [here](#) by Monday, February 9th**. You will receive a confirmation e-mail with arrival and logistical instructions next week. Please expect to arrive at

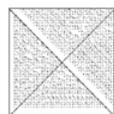
the Summit before 8:00am and depart after 4:30pm.

Due to the high interest in the Summit, we ask that you only register if you are able to attend the full day-long program. If you are not able to attend the full program and would like to just attend the morning session, when we expect President Obama to speak, please e-mail cybersummit@who.eop.gov for the separate RSVP process for morning-only attendees. At this time we are not able to share the full agenda for the Summit. As more details become available they will be posted on WhiteHouse.gov/CyberSummit.

If you have any questions please e-mail cybersummit@who.eop.gov.

Sincerely,

The White House Office of Public Engagement



Non Responsive

-----Original Message-----

From: White House Press Office [noreply@messages.whitehouse.gov]

Sent: Monday, January 12, 2015 06:10 AM Eastern Standard Time

To: Edelman, R. David

Subject: FACT SHEET: Safeguarding American Consumers & Families

THE WHITE HOUSE

Office of the Press Secretary

FOR IMMEDIATE RELEASE

January 12, 2015

**FACT SHEET: Safeguarding American Consumers & Families
President Obama Announces New Privacy Protections for the Digital Age**

Today, President Obama will build on the steps he has taken to protect American companies, consumers, and infrastructure from cyber threats, while safeguarding privacy and civil liberties. These actions have included the President's 2012 comprehensive blueprint for consumer privacy, the BuySecure initiative—launched last year—to safeguard Americans' financial security, and steps the President took earlier this year by creating a working group of senior administration officials to examine issues related to big data and privacy in public services and the commercial sector.

In an increasingly interconnected world, American companies are also leaders in protecting privacy, taking unprecedented steps to invest in cybersecurity and provide customers with precise control over the privacy of their online content. But as cybersecurity threats and identity theft continue to rise, recent polls show that 9 in 10 Americans feel they have in some way lost control of their personal information — and that can lead to less interaction with technology, less innovation, and a less productive economy.

At the Federal Trade Commission offices today, President Obama will highlight measures he will discuss in the State of the Union and unveil the next steps in his comprehensive approach to enhancing consumers' security, tackling identity theft, and improving privacy online and in the classroom. These steps include:

Improving Consumer Confidence by Tackling Identity Theft

- **The Personal Data Notification & Protection Act:** The President is putting forward a new legislative proposal to help bring peace of mind to the tens of millions of Americans whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when their personal information has been exposed, including establishing a 30-day notification requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The proposal also criminalizes illicit overseas trade in identities.

- **Identifying and Preventing Identity Theft:** To give consumers access to one of the best early indicators of identity theft, as well as an opportunity to improve their credit health, JPMorganChase and Bank of America, in partnership with Fair Isaac Corporation (FICO), will join the growing list of firms making credit scores available for free to their consumer card customers. USAA and State Employees' Credit Union will also offer free credit scores to their members, and Ally Financial is further widening the community of companies taking this step by making credit scores available to their auto loan customers. Through this effort over half of all adult Americans with credit scores will now have access to this tool to help spot identity theft, through their banks, card issuers, or lenders.

Safeguarding Student Data in the Classroom and Beyond

- **The Student Digital Privacy Act:** The President is releasing a new legislative proposal designed to provide teachers and parents the confidence they need to enhance teaching and learning with the best technology — by ensuring that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute, builds on the recommendations of the White House Big Data and Privacy review released earlier this year, would prevent companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school — while still permitting important research initiatives to improve student learning outcomes, and efforts by companies to continuously improve the effectiveness of their learning technology products.

- **New Commitments from the Private Sector to Help Enhance Privacy for Students:** Today 75 companies have committed to the cause, signing a pledge to provide parents, teachers, and kids themselves with important protections against misuse of their data. This pledge was led by the Future of Privacy Forum and the Software & Information Industry Association, and today the President challenged other companies to follow their lead.

- **New Tools from the Department of Education to Empower Educators Around the Country and Protect Students:** The Department of Education and its Privacy Technical Assurance Center play a critical role in protecting American children from invasions of privacy. Today, we are announcing a forthcoming model terms of service, as well as teacher training assistance that will enhance our ability to help ensure educational data is used appropriately and in accordance with the educational mission.

Convening the Public and Private Sector to Tackle Emerging Privacy Issues

- **Voluntary Code of Conduct for Smart Grid Customer Data Privacy:** Today the Department of Energy and the Federal Smart Grid Task Force are releasing a new Voluntary Code of Conduct (VCC) for utilities and third parties aimed at protecting electricity customer data — including energy usage information. This Code

reflects a year of expert and public consultation, including input from industry stakeholders, privacy experts, and the public. As companies begin to sign on, the VCC will help improve consumer awareness, choice and consent, and controls on access.

Promoting Innovation by Improving Consumers Confidence Online

• **Consumer Privacy Bill of Rights Legislation:** Online interactions should be governed by clear principles — principles that look at the context in which data is collected and ensure that users' expectations are not abused. Those were the key themes of the Administration's 2012 *Consumer Privacy Bill of Rights*, and today the Commerce Department announced it has completed its public consultation on revised draft legislation enshrining those principles into law. Within 45 days, the Administration will release this revised legislative proposal and today we call on Congress to begin active consideration of this important issue.

These actions build on steps the President has already taken to support consumer privacy and fight identity theft, including:

• **Making Federal Payments More Secure to Help Drive the Market Forward:** In October, as part of his BuySecure Initiative, the President issued an Executive Order laying out a new policy to secure payments to and from the Federal government by applying chip and PIN technology to newly issued and existing government credit cards, as well as debit cards like Direct Express, and upgrading retail payment card terminals at Federal agency facilities to accept chip and PIN-enabled cards. This accompanied an effort by major companies like Home Depot, Target, Walgreens, and Walmart to roll out secure chip and PIN-compatible card terminals in stores across the country.

• **New Measures to Prevent Identity Theft:** The President also announced new steps by the government to assist victims of identity theft, including supporting the Federal Trade Commission in their development of a new one-stop resource for victims at IdentityTheft.gov and expanding information sharing to ensure Federal investigators' ability to regularly report evidence of stolen financial and other information to companies whose customers are directly affected.

###

[Unsubscribe](#)

Non Responsive

From: Cyber Summit [<mailto:cybersummit@who.eop.gov>]
Sent: Friday, February 06, 2015 12:39 PM
To: Ramirez, Edith
Subject: Invitation: White House Cybersecurity Summit on February 13



Greetings,

You are invited to attend the full-day White House Summit on Cybersecurity and Consumer Protection at Stanford University on Friday, February 13th. The Summit will feature remarks by President Obama and bring together major stakeholders on cybersecurity and consumer protection issues to help shape public and private sector efforts to protect American consumers and companies from growing threats to consumers and commercial networks. Lunch will be provided by Stanford University.

From increasing cybersecurity information sharing to improving adoption of more secure payment technologies, here's a look at the topics that panels at the Summit will address:

- Public-Private Collaboration on Cybersecurity
- Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations
- Promoting More Secure Payment Technologies
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation on Cybersecurity
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

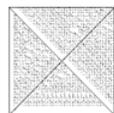
This invitation is non-transferable. **RSVP for the Summit [here](#) by Monday, February 9th**. You will receive a confirmation e-mail with arrival and logistical instructions next week. Please expect to arrive at the Summit before 8:00am and depart after 4:30pm.

Due to the high interest in the Summit, we ask that you only register if you are able to attend the full day-long program. If you are not able to attend the full program and would like to just attend the morning session, when we expect President Obama to speak, please e-mail cybersummit@who.eop.gov for the separate RSVP process for morning-only attendees. At this time we are not able to share the full agenda for the Summit. As more details become available they will be posted on WhiteHouse.gov/CyberSummit.

If you have any questions please e-mail cybersummit@who.eop.gov.

Sincerely,

The White House Office of Public Engagement





The Office of Science and Technology Policy is pleased to invite you to an event at The White House in the morning of **Friday, January 30**.

Details

-

DATE: Friday, January 30, 2015

TIME: Morning TBD

LOCATION: The White House

(Additional logistics will be made available upon receipt of your RSVP).

In order to attend this event, please RSVP by completing the attached form and sending it to Fae Jencks (Fae_M_Jencks@ostp.eop.gov) as soon as possible and no later than **12 PM EST Wednesday, January 28th**.

Please note, **this invitation is non-transferable.**



Non Responsive

From: Cyber Summit [<mailto:cybersummit@who.eop.gov>]
Sent: Friday, February 06, 2015 12:39 PM
To: Ramirez, Edith
Subject: Invitation: White House Cybersecurity Summit on February 13



Greetings,

You are invited to attend the full-day White House Summit on Cybersecurity and Consumer Protection at Stanford University on Friday, February 13th. The Summit will feature remarks by President Obama and bring together major stakeholders on cybersecurity and consumer protection issues to help shape public and private sector efforts to protect American consumers and companies from growing threats to consumers and commercial networks. Lunch will be provided by Stanford University.

From increasing cybersecurity information sharing to improving adoption of more secure payment technologies, here's a look at the topics that panels at the Summit will address:

- Public-Private Collaboration on Cybersecurity

- Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations
- Promoting More Secure Payment Technologies
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation on Cybersecurity
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

This invitation is non-transferable. **RSVP for the Summit [here](#) by Monday, February 9th.** You will receive a confirmation e-mail with arrival and logistical instructions next week. Please expect to arrive at the Summit before 8:00am and depart after 4:30pm.

Due to the high interest in the Summit, we ask that you only register if you are able to attend the full day-long program. If you are not able to attend the full program and would like to just attend the morning session, when we expect President Obama to speak, please e-mail cybersummit@who.eop.gov for the separate RSVP process for morning-only attendees. At this time we are not able to share the full agenda for the Summit. As more details become available they will be posted on WhiteHouse.gov/CyberSummit.

If you have any questions please e-mail cybersummit@who.eop.gov.

Sincerely,

The White House Office of Public Engagement



Non Responsive

From: Edelman, R. David [mailto:Ross_D_Edelman@ostp.eop.gov]
Sent: Monday, January 12, 2015 1:36 PM
To: Ramirez, Edith
Subject: FW: Remarks by the President at the Federal Trade Commission

Congrats on the big day!

From: White House Press Office [mailto:noreply@messages.whitehouse.gov]
Sent: Monday, January 12, 2015 1:21 PM
To: Edelman, R. David
Subject: Remarks by the President at the Federal Trade Commission

<http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd><">

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

January 12, 2015

REMARKS BY THE PRESIDENT
ON PROTECTING CONSUMERS AND FAMILIES IN THE DIGITAL AGE

Federal Trade Commission
Constitution Center
Washington, D.C.

Non Responsive

From: Mielke, Dawn M. [mailto:Dawn_M._Mielke@ostp.eop.gov]
Sent: Tuesday, January 27, 2015 1:22 PM
To: Carter, Monica M.
Subject: RE: Time w/ CTO Team

We are confirmed for 2/5 @ 1 pm. We are coming to your offices, correct? Can you give me a location?

Megan Smith, Chief Technology Officer

Alex Macgillivray, Deputy Chief Technology Officer

From: Carter, Monica M. [mailto:MCARTER@ftc.gov]
Sent: Tuesday, January 27, 2015 1:16 PM
To: Mielke, Dawn M.; Macgillivray, Alexander
Cc: McAllister, Matthew
Subject: RE: Time w/ CTO Team

Good afternoon,

Chairwoman Ramirez will be available to meet on Thursday, February 5, 2015 @1pm. Please confirm date and time, in addition please send me a list of attendees for this scheduled meeting. Thank you so very much.

All my best always,

Monica Carter Etheridge

Executive Assistant to Chairwoman Edith Ramirez

US Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

Email: mcarter@ftc.gov

202-326-2666 (ofc)

202-326-2396 (fax)

"Life isn't about waiting for the storm to pass. It's about learning to dance in the rain."

"When people show you who they are, believe them the first time."

—*Maya Angelou*

From: Mielke, Dawn M. [<mailto:Dawn.M.Mielke@ostp.eop.gov>]

Sent: Tuesday, January 27, 2015 9:54 AM

To: Macgillivray, Alexander; Carter, Monica M.

Cc: McAllister, Matthew

Subject: RE: Time w/ CTO Team

The following times will work for Megan and Alex:

February 5

11:00 am – 2:00 pm

February 19

11:00 am – 2:00 pm

From: Macgillivray, Alexander
Sent: Monday, January 26, 2015 3:26 PM
To: Carter, Monica M.
Cc: McAllister, Matthew; Mielke, Dawn M.
Subject: RE: Time w/ CTO Team

Great. Adding Dawn & Matt to find a time.

-Alex

From: Carter, Monica M. [<mailto:MCARTER@ftc.gov>]
Sent: Monday, January 26, 2015 3:24 PM
To: Macgillivray, Alexander
Subject: FW: Time w/ CTO Team

Good afternoon Alex,

Chairwoman Ramirez's calendar is busy for the next two weeks; please send me some schedule availability on your end for the week of Feb 3-5 and Feb. 17-19. Thank you so very much for your assistance with this meeting request.

All my best,

Monica Carter Etheridge

Executive Assistant to Chairwoman Edith Ramirez

US Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

Email: mcarter@ftc.gov

202-326-2666 (ofc)

202-326-2396 (fax)

"Life isn't about waiting for the storm to pass. It's about learning to dance in the rain."

"When people show you who they are, believe them the first time."

—*Maya Angelou*

From: Ramirez, Edith
Sent: Monday, January 26, 2015 3:01 PM
To: 'Macgillivray, Alexander'
Cc: 'Mielke, Dawn M.'; 'Smith, Megan'; Watson, Shaundra; Carter, Monica M.
Subject: RE: Time w/ CTO Team

Alex,

Thanks for your note. A meeting with you and Megan to discuss your agenda would be terrific. I will have my assistant, Monica Carter, reach out to set something up.

Edith

From: Macgillivray, Alexander [<mailto:amac@ostp.eop.gov>]
Sent: Monday, January 26, 2015 12:22 PM
To: Ramirez, Edith
Cc: Mielke, Dawn M.; Smith, Megan
Subject: Time w/ CTO Team

Chairwoman Ramirez,

It was wonderful to be your guest at the President's privacy focused event on the 12th. Thank you.

If your schedule permits, Megan and I would love to give you and your staff a brief overview of team CTO and the work we have on our agenda. Much of it is consistent with the FTC's strong direction on privacy, competition, and consumer protection work.

-Alex

Non Responsive

Non Responsive

From: Cyber Summit [<mailto:cybersummit@who.eop.gov>]
Sent: Friday, February 06, 2015 12:39 PM
To: Ramirez, Edith
Subject: Invitation: White House Cybersecurity Summit on February 13



Greetings,

You are invited to attend the full-day White House Summit on Cybersecurity and Consumer Protection at Stanford University on Friday, February 13th. The Summit will feature remarks by President Obama and bring together major stakeholders on cybersecurity and consumer protection issues to help shape public and private sector efforts to protect American consumers and companies from growing threats to consumers and commercial networks. Lunch will be provided by Stanford University.

From increasing cybersecurity information sharing to improving adoption of more secure payment technologies, here's a look at the topics that panels at the Summit will address:

- Public-Private Collaboration on Cybersecurity
- Improving Cybersecurity Practices at Consumer-Oriented Businesses and Organizations
- Promoting More Secure Payment Technologies
- Cybersecurity Information Sharing
- International Law Enforcement Cooperation on Cybersecurity
- Improving Authentication: Moving Beyond the Password
- Chief Security Officers' Perspectives: New Ideas on Technical Security

This invitation is non-transferable. **RSVP for the Summit [here](#) by Monday, February 9th**. You will receive a confirmation e-mail with arrival and logistical instructions next week. Please expect to arrive at the Summit before 8:00am and depart after 4:30pm.

Due to the high interest in the Summit, we ask that you only register if you are able to attend the full day-long program. If you are not able to attend the full program and would like to just attend the morning session, when we expect President Obama to speak, please e-mail cybersummit@who.eop.gov for the separate RSVP process for morning-only attendees. At this time we are not able to share the full agenda for the Summit. As more details become available they will be posted on WhiteHouse.gov/CyberSummit.

If you have any questions please e-mail cybersummit@who.eop.gov.

Sincerely,

The White House Office of Public Engagement



Non Responsive

From: Jencks, Fae [mailto:Fae_M_Jencks@ostp.eop.gov]
Sent: Tuesday, January 27, 2015 12:29 PM
To: Jencks, Fae
Subject: INVITATION: White House Event



The Office of Science and Technology Policy is pleased to invite you to an event at The White House in the morning of **Friday, January 30**.

Details

DATE: Friday, January 30, 2015

TIME: Morning TBD

LOCATION: The White House

(Additional logistics will be made available upon receipt of your RSVP).

In order to attend this event, please RSVP by completing the attached form and sending it to Fae Jencks (Fae_M_Jencks@ostp.eop.gov) as soon as possible and no later than **12 PM EST Wednesday, January 28th**.

Please note, **this invitation is non-transferable.**

Non Responsive

From: Jencks, Fae [mailto:Fae_M_Jencks@ostp.eop.gov]
Sent: Tuesday, January 27, 2015 12:29 PM
To: Jencks, Fae
Subject: INVITATION: White House Event



The Office of Science and Technology Policy is pleased to invite you to an event at The White House in the morning of **Friday, January 30**.

Details

-

DATE: Friday, January 30, 2015
TIME: Morning TBD
LOCATION: The White House

(Additional logistics will be made available upon receipt of your RSVP).

In order to attend this event, please RSVP by completing the attached form and sending it to Fae Jencks (Fae_M_Jencks@ostp.eop.gov) as soon as possible and no later than **12 PM EST Wednesday, January 28th**.

Please note, **this invitation is non-transferable.**

R. David Edelman

Senior Advisor for Technology & Economic Policy
direct: (202) 456-7821 | topline: (202) 456-6010

Non Responsive

From: Jencks, Fae [mailto:Fae_M_Jencks@ostp.eop.gov]
Sent: Tuesday, January 27, 2015 12:29 PM
To: Jencks, Fae
Subject: INVITATION: White House Event



The Office of Science and Technology Policy is pleased to invite you to an event at The White House in the morning of **Friday, January 30**.

Details

-

DATE: **Friday, January 30, 2015**

TIME: Morning TBD

LOCATION: The White House

(Additional logistics will be made available upon receipt of your RSVP).

In order to attend this event, please RSVP by completing the attached form and sending it to Fae Jencks (Fae_M_Jencks@ostp.eop.gov) as soon as possible and no later than **12 PM EST Wednesday, January 28th**.

Please note, **this invitation is non-transferable.**

Non Responsive

From: Jencks, Fae [mailto:Fae_M_Jencks@ostp.eop.gov]
Sent: Tuesday, January 27, 2015 12:29 PM
To: Jencks, Fae
Subject: INVITATION: White House Event



The Office of Science and Technology Policy is pleased to invite you to an event at The White House in the morning of **Friday, January 30**.

Details

-

DATE: Friday, January 30, 2015

TIME: Morning TBD

LOCATION: The White House

(Additional logistics will be made available upon receipt of your RSVP).

In order to attend this event, please RSVP by completing the attached form and sending it to Fae Jencks (Fae_M_Jencks@ostp.eop.gov) as soon as possible and no later than **12 PM EST Wednesday, January 28th**.

Please note, **this invitation is non-transferable.**

Non Responsive

Duplicate

To: Ramirez, Edith[eramirez@ftc.gov]
Cc: Watson, Shaundra[SWATSON@ftc.gov]
From: Edelman, R. David
Sent: Thur 1/8/2015 2:24:46 PM
Importance: Normal
Subject: RE: Student Privacy Draft Bill
MAIL_RECEIVED: Thur 1/8/2015 2:24:53 PM

Edith,

(b)(5) Non Responsive

Non Responsive

Non Responsive

Best,

-rD

From: Ramirez, Edith [mailto:eramirez@ftc.gov]
Sent: Thursday, January 08, 2015 1:19 PM
To: Edelman, R. David
Cc: Watson, Shaundra
Subject: RE: Student Privacy Draft Bill

David,

(b)(5)

Non Responsive

Edith

From: Edelman, R. David [mailto:Ross_D_Edelman@ostp.eop.gov]
Sent: Thursday, January 08, 2015 8:35 AM
To: Ramirez, Edith
Cc: Watson, Shaundra
Subject: Student Privacy Draft Bill

DANA ROHRBACHER

48th District, California

WASHINGTON OFFICE:

2300 Rayburn House Office Building
Washington, DC 20515-0548
(202) 225-2415

DISTRICT OFFICE:

101 Main Street, Suite 390
Huntington Beach, CA 92648-6118
(714) 960-6483

<http://rohrbacher.house.gov>



Congress of the United States
House of Representatives

Committees:

FOREIGN AFFAIRS

Chairman, Subcommittee on
Europe, Eurasia, and Emerging Threats
Subcommittee on Asia and the Pacific

SCIENCE, SPACE, AND TECHNOLOGY
(VICE CHAIRMAN)

Subcommittee on Space
Subcommittee on Environment

October 9, 2014

The Honorable Edith Ramirez
Chairwoman, Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

The Honorable William Baer
Assistant Attorney General
U.S. Department of Justice
950 Pennsylvania Ave., NW
Washington, DC 20530

Dear Chairwoman Ramirez and Assistant Attorney General Baer:

I write today to urge that the antitrust enforcement agencies closely examine a proposed \$50 billion merger between French multinational Lafarge and Swiss multinational Holcim, two of the world's largest producers of cement. I ask your agencies to carefully review the likely impact on competition and prices which would result from this European consortium, especially in light of the fact that these two companies have been sanctioned in the past for illegal business practices.

Lafarge and Holcim have long histories of unscrupulous business practices in foreign nations. Both companies were fined for anticompetitive business practices in Brazil and the European Union. Lafarge was fined €250 million for price fixing in 2002. I am also aware of allegations that Lafarge conspired with the Government of Honduras to block a US competitor from the Honduran and Central American markets through predatory pricing.

The proposed merger has serious implications for competition in this vital industry and for construction costs in the United States. For these reasons, I urge your agencies to examine the proposed merger very closely.

Sincerely,

Dana Rohrabacher
Chairman
Subcommittee on Europe, Eurasia, and Emerging
Threats
House Committee on Foreign Affairs

PATRICK J. LEAHY, VERMONT, CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA

United States Senate

COMMITTEE ON THE JUDICIARY

WASHINGTON, DC 20510-6275

KRISTINE J. LUCIUS, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

October 17, 2014

The Honorable Edith Ramirez
Chairwoman, Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairwoman Ramirez:

We are writing to you regarding the proposed acquisition of US Foods by Sysco currently being reviewed by the Federal Trade Commission. While we take no position about the legality of the merger under the antitrust laws, we do think it raises important competition issues the Commission should carefully review and closely scrutinize.

The \$231 billion foodservice distribution industry touches every single American consumer who eats meals away from home. Large and small chain restaurants, mom and pop cafés, schools, hospitals, corporate cafeterias, and stadiums all rely on companies like Sysco and US Foods for food and dining supplies. A competitive market for distribution services is essential to ensuring consumers receive the highest quality products and services at the best prices.

If consummated, this merger would combine Sysco and US Foods, the largest and second-largest foodservice companies in the country. The combined entity would control approximately 27 percent of the market by revenue. The next largest competitor would be about one-fifth its size with a five percent market share. According to the American Antitrust Institute, the combined entity would have an estimated 54 percent market share of “broadline service,” *i.e.*, providing food and dining supplies for customers ranging from independent mom and pop restaurants to large and small chain restaurants, schools, hospitals, corporate cafeterias, and stadiums. Critics of this transaction worry that by consolidating the market through a merger of the top two competitors, consumers will face higher prices and reduced quality of service. They also worry that some customers will not consider regional foodservice competitors as adequate substitutes for a national broadline company—leading, perhaps, to a discrete market for national broadline service over which the combined entity would enjoy a monopoly.

Sysco and US Foods, however, contend that the merger will have a number of competitive benefits. Most importantly, they believe they can combine their complementary strengths and achieve \$600 million in cost savings, while their increased size will give them the ability to negotiate lower prices for their customers. The companies also claim that the foodservice industry is and would remain highly competitive after a merger. It is their view that they face intense competition from local and regional foodservice companies and expanding self-service wholesale food stores, and that that competition will prevent them from raising prices or diminishing the quality of their products. They believe, moreover, that as a practical matter a

combined entity would not be able to raise prices to an anticompetitive level because, in the low-margin foodservice distribution business, customers have the bargaining power and ability to shift portions of their business to regional and local competitors in response to price increases.

We urge you to closely look at whether regional competitors can be relied upon to counter any market power that Sysco and US Foods may achieve through the merger. Critics contend that regional broadline foodservice providers lack the scale to be able to competitively price against Sysco and US Foods, that switching costs for customers could be high, and that piecing together regional companies is inefficient and would not outweigh the benefits. In particular, we hope you will examine: (1) whether there is a distinct market for national broadline service; (2) the overlap between local and regional markets; and (3) whether adequate competition depends on the willingness of regional foodservice companies to combine or expand their activities and, if so, how likely they are to take those steps successfully. We also hope you will consider the companies' central contention that the proposed merger will result in significant cost savings and price competition that will benefit the many small businesses that use broadline companies.

This is a critically important merger because it has the potential to impact so many food establishments, both large and small, and ultimately affect the prices consumers pay every time they go out to eat. Without reaching any conclusion about whether the Sysco/US Foods transaction would create market dominance or substantial harm to competition, we believe it is essential that the FTC scrutinize the proposed transaction and give careful attention to these concerns.

Thank you for your attention to this matter.

Sincerely,



Amy Klobuchar
Chairman, Subcommittee on
Antitrust, Competition Policy
and Consumer Rights



Mike Lee
Ranking Member, Subcommittee on
Antitrust, Competition Policy
and Consumer Rights

United States Senate

WASHINGTON, DC 20510

December 1, 2014

COMMITTEES:
BANKING
DEMOCRATIC POLICY & COMMUNICATIONS
FINANCE
JUDICIARY
RULES

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Dear Chairwoman Ramirez,

Thank you for your continued commitment to protecting American consumers, especially in the area of data privacy and security. I'm sure you were as disturbed as I was to read recent reports of hackers exploiting new features in televisions, cameras and even baby monitors in order to break into the home systems of users and spy on unsuspecting consumers, and broadcasting these private video streams over a public Russian website, www.insecam.cc. For any of these devices to secretly function as a sort of spycam would violate a basic expectation of privacy in the American home. These types of privacy breaches could lead to voyeurism, robbery and even blackmail.

As technology has advanced in recent years, we are connected in ways that were previously unimaginable. Televisions now have Wi-Fi, cameras, and other features similar to those of a computer, and are able to complete new and exciting tasks: surfing the internet, making calls, streaming videos and more. New baby monitors allow video to be streamed to the web, allowing parents to easily check in on their young children, while computer webcams have allowed families to stay in touch no matter where in the world they may be. These types of advances can dramatically improve the day to day lives of the American consumers. What has not changed, however, is that Americans expect that when they turn on the television or log in online to check on their baby, they are adequately protected from hackers that would attempt to exploit otherwise unaware citizens.

Under your leadership, the FTC has been at the forefront of helping industry to negotiate the complicated balance of privacy and innovation with internet-enabled consumer devices. You have run important workshops on these issues to help generate rules of the road. Perhaps more importantly, you have appropriately used your enforcement authority against those companies that misrepresent the security of their devices, such as TRENDnet.

As you continue your diligent efforts in the privacy and security world, I ask that the FTC pay specific attention to the particular issue of camera-enabled devices being vulnerable to hackers. I am particularly concerned that the practice of using default passwords with devices can convey a false sense of security. As we saw with the Russian website www.insecam.cc, many users don't change the default password leaving them with the belief that they are protected, but just as vulnerable to hackers as if they had no password at all. One example, therefore, of a change I



believe should be made to improve device security would be to eliminate default passwords and require users to establish a unique code on set up.

I hope that you will do what you can to work with industry to adopt this and other safety and security standards so that hackers cannot break into our devices. The Federal Trade Commission has been an indispensable partner in the fight to protect consumer security, and I am confident you share my view that it is imperative that we protect people that purchase televisions, computers or baby monitors with these features from being hacked or spied on, and possibly divulging information they intend to keep private.

Thank you and I look forward to working with you on this important issue.

Sincerely,



Charles E. Schumer
United States Senator

PATRICK J. LEAHY, VERMONT, CHAIRMAN

DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT
MAZIE HIRONO, HAWAII

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TED CRUZ, TEXAS
JEFF FLAKE, ARIZONA

KRISTINE J. LUCIUS, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

United States Senate

COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

October 29, 2014

The Honorable Edith Ramirez, Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Dear Chairwoman Ramirez:

We are writing to request the prompt release of the 2013 fiscal year staff report on agreements filed with the Federal Trade Commission under the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, as well as a timely 2014 fiscal year staff report.

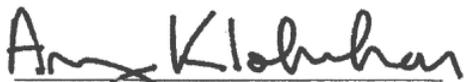
Since 2004, the Federal Trade Commission has released annual reports summarizing agreements between brand and generic medical manufacturers, providing important information on the use of pay-for-delay provisions in patent dispute resolutions. Pay-for-delay agreements, monetary settlements made by brand name drug companies to generic drug companies in exchange for delaying the marketing of generic competitors, deny consumer access to more affordable alternatives to brand medications. The FTC estimated that these anticompetitive deals result in consumers and taxpayers paying an additional \$3.5 billion in higher drug costs every year.

It is critical to have access to these numbers in order to better understand the impact of “pay-for-delay” agreements. In July 2013, the Judiciary Committee Subcommittee on Antitrust, Competition Policy, and Consumer Rights held a hearing on pay-for-delay deals where Chairwoman Ramirez stated that this issue is a top priority for the agency. We applaud the efforts of the Federal Trade Commission to make this agreement information available, and seek your continued input on the matter. Having up-to-date numbers is an important part of developing legislation that would curb this anticompetitive behavior.

It is also important to understand how the 2013 Supreme Court case *FTC v. Actavis* has impacted patent dispute resolution, as well as the steps the FTC has taken since the decision to challenge pay-for-delay settlements. While the decision made clear that these agreements are subject to antitrust scrutiny, you have stated that the litigation is both time and resource intensive, and lacks a bright line standard. Your numbers from the 2012 staff report showed a dramatic increase in the number of these pay-for-delay agreements; release of the 2013 and 2014 numbers will help Congress understand whether the Court’s decision has altered the behavior of drug manufacturers, and what legislative reforms are currently needed.

We look forward to working with you to protect consumers and encourage competitive behavior in the medication marketplace.

Sincerely,


Senator Amy Klobuchar


Senator Chuck Grassley

United States Senate

WASHINGTON, DC 20510

December 08, 2014

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: AB Acquisition LLC and Safeway Inc. Merger

Dear Chairwoman Ramirez:

We are writing regarding the potential impact of the proposed merger between AB Acquisition LLC and Safeway Inc. We strongly support the role of the Federal Trade Commission (FTC) in protecting consumers' interests and enforcing anti-trust laws during mergers. We also believe it is crucial that the FTC's review and approval process ensures that communities are not inadvertently harmed in the process.

It is our understanding that due to significant overlap between the two store chains, in some states there could be store closures and divestitures to avoid anti-trust concerns. These actions could have serious consequences for small communities, including in Baker County, Oregon, without additional measures that would maintain the current access to grocery stores and competition.

We have recently heard from the Baker County Board of Commissioners and the Baker City Council who have expressed concerns that the review process may result in the closure of one of only two large grocery stores in Baker County. Baker County is home to over 16,000 residents and it would be difficult for only one grocery store to serve the community's needs, particularly in a noncompetitive environment. If divestiture is necessary, requiring that one of the stores be sold to another grocer would both help maintain a competitive marketplace and preserve options for Baker County residents.

As the FTC continues its review process, we urge you to closely examine the effects of the merger on the residents of communities where closures or divestitures may take place and to ensure that any necessary changes will not inadvertently leave communities without adequate resources.

Thank you for your attention to this matter.

Sincerely,



Jeffrey A. Merkley
United States Senator



Ron Wyden
United States Senator

CHARLES J. "CHUCK" FLEISCHMANN
3RD DISTRICT, TENNESSEE

COMMITTEE ON APPROPRIATIONS
SUBCOMMITTEE ON ENERGY AND WATER
SUBCOMMITTEE ON LABOR, HEALTH AND HUMAN
SERVICES, EDUCATION AND RELATED AGENCIES
SUBCOMMITTEE ON HOMELAND SECURITY



Congress of the United States
House of Representatives
Washington, DC 20515-4203

WASHINGTON OFFICE
230 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3271 (202) 225-3484 (FAX)

DISTRICT OFFICES
FEDERAL COURTHOUSE, SUITE 126
800 GEORGIA AVENUE
CHATTANOOGA, TN 37402
(423) 756-2342 (423) 766-8813 (FAX)

200 ADMINISTRATION ROAD, SUITE 100
P.O. BOX 2801
OAK RIDGE, TN 37830
(865) 576-1976 (865) 576-3221 (FAX)

6 EAST MADISON AVENUE COURTHOUSE
ATHENS, TN 37303-4297

January 27, 2015

1401175

Edith Ramirez, Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairwoman Ramirez:

I am writing to you today in regards to concerns that have been raised by my constituents regarding price increases within the generic prescription drug market. These price increases could significantly affect both people and businesses within my district, and I would like to make the Federal Trade Commission (FTC) aware of the merit of these concerns. It is my hope that the FTC may be able to assist me in understanding these price changes as well as inform me about any prior activity regarding price volatility that FTC has been made aware of.

The alarming rise and volatility in the prices of generic drugs has become a national healthcare issue. Traditionally, generic drugs supply a cheaper, more affordable option to patients on lean budgets. Truveris, a leader in health information technology for pharmacy pricing, reports most generic drug prices increase by a manageable 10% a year; however, there are many generic drugs that have seen their prices increase by more than 1,000% in the last year. According to the Healthcare Supply Chain Association (HSCA), the price of a 100-count bottle of 2mg albuterol sulfate tablets, used to treat asthma, increased by 4,014% in a span of six months. Digoxin, a drug used to treat irregular heartbeats, saw an 884% increase. These are common generic drugs are essential to the daily lives of many of my constituents. In the case of the blood pressure medication captopril, the drug underwent a 17,000% price increase over the last 12 months.

As prices climb, some retail chains have begun dropping drugs from their generic drug program, leaving patients with fewer affordable options. According to the Food and Drug Administration (FDA), approximately 80% of all filled prescriptions are generic drugs. The Generic Pharmaceutical Association (GPA) estimates generic drugs save over \$200 billion in healthcare costs per year. This makes affordable generic drug access vital to the health of our communities. I am concerned that in some cases, these price increases can prevent patients from obtaining critically needed pharmaceuticals. Consumers without insurance plans or with high-deductible plans could be particularly affected.

FEDERAL TRADE COMMISSION
2015 JAN 29 PM 4:46
CONG. CORRES. BRANCH

The rise in costs not only affects prices and access for patients, but particularly hurts older citizens and small community pharmacies. Increases in insurance premiums are passed on to the patient, and small independent pharmacies also stand to lose as it is difficult for them to absorb price shocks without dropping the drug completely or raising prices.

It is important that the FTC carefully examine this issue so that Americans are able to access affordable generic prescription medications that meet their healthcare needs. I look forward to your response and your continued attention to matters such as this.

Sincerely,

A handwritten signature in black ink, appearing to read "Chuck Fleischmann", with a long horizontal flourish extending to the right.

Chuck Fleischmann
Member of Congress

JOSEPH P. KENNEDY III
4TH DISTRICT, MASSACHUSETTS

COMMITTEE ON FOREIGN AFFAIRS
SUBCOMMITTEE ON MIDDLE EAST AND NORTH AFRICA
SUBCOMMITTEE ON TERRORISM, NONPROLIFERATION,
AND TRADE

COMMITTEE ON SCIENCE, SPACE, AND
TECHNOLOGY
SUBCOMMITTEE ON ENERGY
SUBCOMMITTEE ON SPACE

Congress of the United States
House of Representatives
Washington, DC 20515-2104

1218 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-5931

DISTRICT OFFICES:
29 CRAFTS STREET
SUITE 375
NEWTON, MA 02458
(617) 332-3333

8 NORTH MAIN STREET
SUITE 200
ATTLEBORO, MA 02703
(508) 431-1110

November 21, 2014

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Federal Trade Commission
Received

DEC 1 - 2014

Chairwoman Ramirez

Dear Chairwoman Ramirez:

I write today on behalf of HeyWire Business, a company located in Brookline, Massachusetts that requested I bring their concerns to the attention of both the Federal Trade Commission and the Federal Communications Commission.

Enclosed, please find a copy of a letter that I received from HeyWire Business, a company specializing in telecommunications and text services. The company reports that Verizon, AT&T, Sprint, T-Mobile, and US Cellular are engaging in anti-competitive practices that "stifle innovation, development of new technologies and services that benefit both consumers and businesses." Specifically, the letter expresses concerns with conflicts of interest, gatekeeper fees, access, and intentional disruptions.

I share your commitment to an open, competitive marketplace that promotes competition and fosters economic growth for America's small businesses and start-up companies, and I thank you for your attention to this matter.

Sincerely,


Joseph P. Kennedy, III
Member of Congress

FEDERAL TRADE COMMISSION
2014 DEC 05 PM 1:26
CONG. CORRES. BRANCH



August 8, 2014

Office of Congressman Joseph Kennedy
1218 Longworth House Office Building
Washington, DC 20515-2104

Representative Kennedy,

I am CEO of MediaFriends Inc., dba HeyWire Business, located in Cambridge MA, with many of our employees living in your district. My CTO and I met you last year in your offices to discuss technology companies in Massachusetts. We shared with you back then some initial concerns regarding carrier behavior, which have only gotten more serious over time.

HeyWire Business has been recognized as one of the hottest companies by the Mass Technology Leadership Council (Mass TLC) and The Massachusetts Innovation Technology Exchange (MITX), and has grown headcount by 35% over the last two years. We have been at the forefront of driving innovation with our mobile enterprise messaging platform enabling smartphone, tablet and computer messaging. We have been recognized as an industry leader: recently *featured in Forbes, Inc., Bloomberg Business, and the Boston Business Journal.*

I am writing to ask for your help in addressing discriminatory, anti-competitive business practices that we are suffering at the hands of the large, legacy telecom providers: *Verizon, AT&T, Sprint, T-Mobile and US Cellular.* This is a serious issue impacting us and other hi-tech companies throughout the industry.

These telecommunications incumbents have used their position as "gatekeepers" to block commonly accepted business practices of equal access and neutrality, effectively establishing a consortium that is now crippling our ability to develop new products. It is stifling innovation, development of new technologies and services that benefit consumers and businesses.

Specific anti-competitive actions by the carriers include:

- 1) **Gatekeeper Fees:** Applying discriminatory and arbitrary "fees" on our company. The consortium does *not* apply these fees to each other. In addition to hurting our business, our employees, and other technology businesses, it ultimately hurts the consumer through increasing our costs arbitrarily for no reason other than what is best perceived as discriminatory against a competitive threat. *This anti-competitive practice clearly is aimed at crippling our ability to bring forward telecom solutions that will benefit the consumer.*
- 2) **Access Denial.** The consortium has refused to provide picture messaging interconnection (the ability for anyone to send or receive picture text messages to anyone else) – thus limiting our ability to offer this valued service to our customers.



3) **Purposeful Interruption.** We have suffered interruptions to our services without warning. In one recent incident, our service with *Verizon* text messaging for 800 toll free numbers was terminated without notice or warning, disrupting our business and our customer's business, which in turn affected the end consumer, for weeks.

Summary

These actions are discriminatory, anti-competitive, present a real threat to our company and the ability of technology companies like ours to compete. Based on your established advocacy for the citizens of your district, the technology sector, consumer rights, and your sponsorship of H.R. 3690, we are asking you to take action to support us in challenging these discriminatory practices by this telecom consortium.

I am requesting your help to please ask the FCC & FTC to look into this matter and take actions to help stop this monopolistic type of behavior that is hurting innovative and entrepreneurial companies, their employees and consumers. Attached are sample letters for your review.

Please let me know if I can provide you with any additional information and/or would be happy to meet with you or your staff.

Regards,

A handwritten signature in black ink, appearing to read "Meredith Flynn-Ripley". The signature is fluid and cursive, with a large loop at the end.

Meredith Flynn-Ripley
CEO

MediaFriends, Inc., dba HeyWire

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

January 20, 2015

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Ave NW
Washington, D.C. 20580

Dear Chairwoman Ramirez:

I write to request a confidential staff briefing on the Federal Trade Commission's forthcoming report on the Internet of Things. I hope to set up a briefing at your earliest convenience, and if possible, on Friday January 23, 2014, at 4:00 P.M.

I understand the sensitivity of discussing such matters, and neither I nor my staff will disclose any non-public information that your staff provides during the briefing.

Thank you for your assistance in this matter.

Very respectfully yours,



JOHN THUNE
CHAIRMAN

MICHAEL S. LEE
UTAH

BOYD C. MATHESON
CHIEF OF STAFF

United States Senate

WASHINGTON, DC 20510-4404

COMMITTEES:
JUDICIARY
ENERGY AND
NATURAL RESOURCES
ARMED SERVICES
JOINT ECONOMIC
COMMITTEE

5 February 2015

Hon. Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Ave. N.W., Ste. 444
Washington, D.C. 20580

Dear Chairwoman Ramirez:

I write to request that knowledgeable members of the FTC staff provide our Subcommittee staff with a confidential briefing about the FTC's investigation into Sysco Corp.'s acquisition of U.S. Foods Inc.

I understand the sensitivity of discussing potential or pending investigations. My staff and I will therefore ensure that any non-public information that your staff provides during the briefing will not be shared with anyone outside the Subcommittee. If you require further confidentiality assurances, we will do our best to accommodate you.

Thank you very much for your assistance in this matter.

Sincerely,



Michael S. Lee
Chairman
Subcommittee on Antitrust,
Competition Policy, and Consumer Rights

JOHN THUNE, SOUTH DAKOTA, CHAIRMAN

ROGER WICKER, MISSISSIPPI
ROY BLUNT, MISSOURI
MARCO RUBIO, FLORIDA
KELLY AYOTTE, NEW HAMPSHIRE
TED CRUZ, TEXAS
DEB FISCHER, NEBRASKA
JERRY MORAN, KANSAS
DAN SULLIVAN, ALASKA
RON JOHNSON, WISCONSIN
DEAN HELLES, NEVADA
CORY GARDNER, COLORADO
STEVE DAINES, MONTANA

BILL NELSON, FLORIDA
MARIA CANTWELL, WASHINGTON
CLAIRE McCASKILL, MISSOURI
AMY KLOBUCHAR, MINNESOTA
RICHARD BLUMENTHAL, CONNECTICUT
BRIAN SCHATZ, HAWAII
EDWARD MARKEY, MASSACHUSETTS
CORY BOOKER, NEW JERSEY
TOM UDALL, NEW MEXICO
JOE MANCHIN II, WEST VIRGINIA
GARY PETERS, MICHIGAN

DAVID SCHWEITERT, STAFF DIRECTOR
KIM LIPSKY, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON COMMERCE, SCIENCE,
AND TRANSPORTATION

WASHINGTON, DC 20510-6125

WEBSITE: <http://commerce.senate.gov>

February 6, 2015

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairwoman Ramirez:

We write this letter to you requesting that the Federal Trade Commission (FTC) investigate Verizon's disclosures to wireless customers with regard to its mobile tracking technology, colloquially known as a "supercookie." Specifically, numerous press outlets reported that the online advertising company, Turn, used Verizon's network-based persistent identifier to regenerate browser cookies that consumers had deleted from their mobile devices. On January 29, we sent a letter to Verizon Chairman and CEO, Lowell C. McAdam, asking (among other things):

"What, if any information and disclosures does Verizon provide its wireless customers about how third-party companies use or can use Verizon's mobile tracker? How has the policy changed, if at all, given press accounts about Turn?"

In response, the company sent us its "Full Privacy Policy" but did not provide any other public disclosures or information provided to wireless customers. Verizon also did not answer whether its policy had changed upon discovery of Turn's practices.

We have attached the "Full Privacy Policy" for your review and ask that you further scrutinize all public and customer disclosures and information relevant to the use of its supercookie by third parties, including disclosures made before discovery of Turn's practices.

Honorable Ramirez
February 6, 2015
Page 2 of 2

We appreciate the Commission's long and distinguished enforcement actions against companies that engage in deceptive practices and violate consumer privacy. Thank you for your attention to this matter.

Sincerely,



Bill Nelson
Ranking Member
Committee on Commerce,
Science, and Transportation



Richard Blumenthal
Ranking Member, Subcommittee on
Consumer Protection, Product Safety,
Insurance, and Data Security



Edward J. Markey
Member

CC: The Honorable John Thune

United States Senate

WASHINGTON, DC 20510

14011332

November 12, 2014

FEDERAL TRADE COMMISSION
2014 NOV 12 AM 11:36
CONG. CORRES. BRANCH

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580

Dear Chairwoman Ramirez:

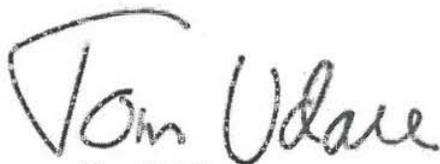
We write to ask that the Federal Trade Commission give due consideration to a request from Plant Oil Powered Diesel Fuel Systems, Inc. ("POP Diesel") for an investigation of alleged anticompetitive practices related to the development of fuel quality standards.

POP Diesel is a New Mexico-based company that manufactures and sells equipment to enable any diesel engine to operate on 100 percent plant oil fuel. In 2013, POP Diesel won approval from the Environmental Protection Agency (EPA) to sell straight vegetable oil as a fuel for engines equipped with POP Diesel technology. The company aims to establish the first nationwide network of filling stations for jatropha plant oil.

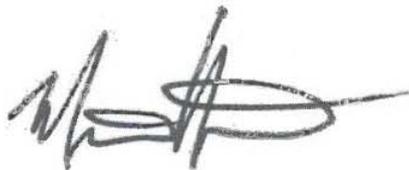
POP Diesel recently requested that the Commission investigate the setting of fuel quality standards and specifications by ASTM International that exclude pure plant oil for use in certain engines. Such technical standards are often incorporated into laws and regulations promulgated by state and Federal agencies, and the exclusion of entirely plant-based oils from these standards could inhibit their adoption and lead to reduced competition in the fuels marketplace.

We therefore ask that you fully and carefully consider POP Diesel's request and take appropriate action if the Commission finds a violation of Section 5 of the Federal Trade Commission Act (15 U.S.C 45).

Sincerely,



Tom Udall
United States Senator



Martin Heinrich
United States Senator

DARRELL E. ISSA, CALIFORNIA
CHAIRMAN

JOHN L. MICA, FLORIDA
MICHAEL R. TURNER, OHIO
JOHN J. DUNCAN, JR., TENNESSEE
PATRICK T. MCHEENRY, NORTH CAROLINA
JIM JORDAN, OHIO
JASON CHAFFETZ, UTAH
TIM WALBERG, MICHIGAN
JAMES LANKFORD, OKLAHOMA
JUSTIN AMASH, MICHIGAN
PAUL A. GOSAR, ARIZONA
PATRICK MEEHAN, PENNSYLVANIA
SCOTT DESJARLAIS, TENNESSEE
TREY GOWDY, SOUTH CAROLINA
BLAKE FARENTHOLD, TEXAS
DOC HASTINGS, WASHINGTON
CYNTHIA M. LUMMIS, WYOMING
ROB WOODALL, GEORGIA
THOMAS MASSIE, KENTUCKY
DOUG COLLINS, GEORGIA
MARK MEADOWS, NORTH CAROLINA
KERRY L. BENTIVOGLIO, MICHIGAN
RON DESANTIS, FLORIDA

LAWRENCE J. BRADY
STAFF DIRECTOR

ONE HUNDRED THIRTEENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
<http://oversight.house.gov>

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
STEPHEN F. LYNCH, MASSACHUSETTS
JIM COOPER, TENNESSEE
GERALD E. CONNOLLY, VIRGINIA
JACKIE SPEIER, CALIFORNIA
MATTHEW A. CARTWRIGHT, PENNSYLVANIA
L. TAMMY DUCKWORTH, ILLINOIS
ROBIN L. KELLY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
PETER WELCH, VERMONT
TONY CARDENAS, CALIFORNIA
STEVEN A. HORSFORD, NEVADA
MICHELLE LUJAN GRISHAM, NEW MEXICO
VACANCY

Federal Trade Commission
Received

DEC 5 - 2014

Chairwoman Ramirez

December 1, 2014

The Honorable Edith Ramirez
Chairwoman
U.S. Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580

Dear Ms. Ramirez:

The Committee on Oversight and Government Reform has been investigating the activities of Tiversa, Inc., a Pittsburgh-based company that purportedly provides peer-to-peer intelligence services. The Federal Trade Commission has relied on Tiversa as a source of information in its enforcement action against LabMD, Inc., a Georgia-based medical testing laboratory. The Committee has obtained documents and information indicating Tiversa failed to provide full and complete information about work it performed regarding the inadvertent leak of LabMD data on peer-to-peer computer networks. In fact, it appears that, in responding to an FTC subpoena issued on September 30, 2013, Tiversa withheld responsive information that contradicted other information it did provide about the source and spread of the LabMD data, a billing spreadsheet file.

Despite a broad subpoena request, Tiversa provided only summary information to the FTC about its knowledge of the source and spread of the LabMD file.

Initially, Tiversa, through an entity known as the Privacy Institute, provided the FTC with information about peer-to-peer data leaks at nearly 100 companies, including LabMD.¹ Tiversa created the Privacy Institute for the specific purpose of providing information to the FTC. Despite Tiversa's claims that it is a trusted government partner, it did not want to disclose that it provided information to the FTC.²

After the FTC filed a complaint against LabMD, the agency served Tiversa with a subpoena for documents related to the matter. Among other categories of documents, the subpoena requested "all documents related to LabMD."³ In a transcribed interview, Alain Sheer,

¹ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Robert Boback, Chief Executive Officer, Tiversa, Inc., Transcript at 42 (June 5, 2014) [hereinafter Boback Tr.].

² See Tiversa, Industry Outlook, Government/Law Enforcement, available at <http://tiversa.com/explore/industry/gov> (last visited Nov. 21, 2014); Boback Tr. at 42-43.

³ Fed. Trade Comm'n, Subpoena to Tiversa Holding Corp. (Sept. 30, 2013) [hereinafter Tiversa FTC Subpoena].

an attorney with the FTC's Bureau of Consumer Protection, told the Committee that the FTC did not narrow the subpoena for Tiversa. Sheer stated:

Q This is the specifications requested of Tiversa. No. 4 requests all documents related to LabMD. Do you know if Tiversa produced all documents related to LabMD?

A I am not sure what your question is.

Q Let me ask it a different way. Was the subpoena narrowed in any way for Tiversa?

A Not that I am aware of.⁴

In total, Tiversa produced 8,669 pages of documents in response to the FTC's subpoena. Notably, the production contained five copies of the 1,718-page LabMD Insurance Aging file that Tiversa claimed to have found on peer-to-peer networks and only 79 pages of other materials, none of which materially substantiated Tiversa's claims about the discovery of the file.

The information Tiversa gave the FTC included the IP address from which Tiversa CEO Robert Boback has claimed the company first downloaded the LabMD file, as well as other IP addresses that Tiversa claims also downloaded the file. The origin of the IP address from which Tiversa first downloaded the LabMD file was in dispute in other litigation between LabMD and Tiversa. On numerous occasions, including before the FTC, Boback maintained that Tiversa first downloaded the LabMD file from an IP address in San Diego, California. Boback stated:

Q What is the significance of the IP address, which is 68.107.85.250?

A That would be the IP address that we downloaded the file from, I believe.

Q Going back to CX 21. Is this the initial disclosure source?

A If I know that our initial disclosure source believed that that was it, yes. I don't remember the number specifically, but if that IP address resolves to San Diego, California, then, yes, that is the original disclosure source.

Q When did Tiversa download [the LabMD file]?

A I believe it was in February of 2008.⁵

⁴ H. Comm. on Oversight & Gov't Reform, Transcribed Interview of Alain Sheer, Fed. Trade Comm'n, Transcript at 147 (Oct. 9, 2014).

⁵ In the matter of LabMD, Inc., Deposition of Robert J. Boback, CEO, Tiversa, transcript at 24-25 (Nov. 21, 2013) [hereinafter Boback Nov. 2013 FTC Tr.].

Boback also testified that Tiversa performed an investigation into the LabMD file at the request of a client.⁶ In the course of this investigation, Tiversa concluded that an IP address in Atlanta, Georgia, where LabMD was headquartered, was the initial disclosure source of the document. Boback stated:

Q There is an IP address on the right-hand side, it is 64.190.82.42. What is that?

A That, if I recall, is an IP address that resolves to Atlanta, Georgia.

Q Is that the initial disclosure source?

A We believe that it is the initial disclosure source, yes.

Q And what is that based on?

A The fact that the file, the 1,718 file, when we searched by hash back in that time for our client, we received a response back from 64.190.82.42 suggesting that they had the same file hash as the file that we searched for. We did not download the file from them.

* * *

Q So, I think you are telling me that chronologically this was the first other location for that file in juxtaposition of when you found the file at 68.107.85.250?

A We know that the file in early February, prior to this February 25 date, was downloaded from the 68.107.85.250. Upon a search to determine other locations of the file across the network, it appears that on 2/25/2008 we had a hash match search at 64.190.82.42, which resolved to Atlanta, which led us to believe that without further investigation, that this is most likely the initial disclosing source.

Q What other information do you have about 64.190.82.42?

A I have no other information. I never downloaded the file from them. They only responded to the hash match.⁷

Boback's testimony before the FTC in November 2013 made clear that Tiversa first downloaded the LabMD file from an IP address in San Diego, California, in February 2008, that it only identified LabMD as the disclosing source after performing an investigation requested by a client, and that it never downloaded the file from LabMD.

⁶ Boback Nov. 2013 FTC Tr. at 72-73 ("In 2008, when working for another client, we were attempting to identify the original disclosure source of the file that we discovered from 1 the San Diego IP address.").

⁷ Boback Nov. 2013 FTC Tr. at 41.

Tiversa withheld responsive documents from the FTC, despite the issuance of the September 2013 subpoena. These documents contradict the account Boback provided to the FTC.

On June 3, 2014, the Committee issued a subpoena to Tiversa requesting, among other information, “[a]ll documents and communications referring or relating to LabMD, Inc.”⁸ This request was very similar to the FTC’s request for “all documents related to LabMD.”⁹ Despite nearly identical requests from the FTC and the Committee to Tiversa, Tiversa produced numerous documents to the Committee that it does not appear to have produced to the FTC. Information contained in the documents Tiversa apparently withheld contradicts documents and testimony Tiversa did provide to the FTC.

An internal Tiversa document entitled “Incident Record Form,” dated April 18, 2008, appears to be the earliest reference to the LabMD file in Tiversa’s production to the Committee.¹⁰ This document states that on April 18, 2008, Tiversa detected a file “disclosed by what appears to be a potential provider of services for CIGNA.”¹¹ The Incident Record described the document as a “single Portable Document Format (PDF) that contain[ed] sensitive data on over 8,300 patients,” and explained that “[a]fter reviewing the IP address, resolution results, meta-data and other files, Tiversa believes it is likely that Lab MD near Atlanta, Georgia is the disclosing source.”¹² The name of the file was “insuranceaging_6.05.071.pdf,” which is the same name as the file in question in the FTC proceeding. According to the Incident Record, the IP address disclosing the file was 64.190.82.42—later confirmed to be a LabMD IP address.¹³ Upon learning about the file, CIGNA, a Tiversa client, “asked Tiversa to perform Forensic Investigation activities” on the insurance aging file to determine the extent of proliferation of the file over peer-to-peer networks.¹⁴

An August 2008 Forensic Investigation Report provided the analysis CIGNA requested. This report identified IP address 64.190.82.42—the Atlanta IP address—as proliferation point zero, and the “original source” of the Incident Record Form.¹⁵ A spread analysis included in the August 2008 forensic report stated that the file had been “observed by Tiversa at additional IP addresses” but made clear that Tiversa had not downloaded the file from either additional source because of “network constraint and/or user behavior.”¹⁶ Thus, according to this report, Tiversa had only downloaded the LabMD file from one source in Atlanta, Georgia by August 2008. This contradicts Boback’s testimony that Tiversa first downloaded the LabMD file from an IP address

⁸ H. Comm. on Oversight & Gov’t Reform, Subpoena to Robert Boback, Chief Exec. Officer, Tiversa, Inc. (June 3, 2014).

⁹ Tiversa FTC Subpoena.

¹⁰ Tiversa Incident Record Form, ID # CIG00081 (Apr. 18, 2008).

¹¹ *Id.*

¹² *Id.* (emphasis added).

¹³ *Id.*

¹⁴ Tiversa, Forensic Investigation Report for Ticket #CIG00081 (Aug. 12, 2008). This letter uses the phrase “forensic report” to describe this and a second report created by Tiversa about the LabMD file because that is the title used by Tiversa. It is not clear what, if any, forensic capabilities Tiversa possesses.

¹⁵ *Id.*

¹⁶ *Id.*

in San Diego, California. If Tiversa had in fact downloaded the LabMD file from a San Diego IP address in February 2008, then that fact should be included in this 2008 forensic report. It is not.

One of the two additional IP addresses is located in San Diego, California. It is a different IP address, however, than the one from which Tiversa claims to have originally downloaded the file.¹⁷ Further, Tiversa did not observe that this San Diego IP address possessed the LabMD file until August 5, 2008.¹⁸ Thus, according to this report, Tiversa did not observe any San Diego IP address in possession of the LabMD file until August 2008. Again, the report stands in stark contrast to Boback's testimony that Tiversa first downloaded the LabMD file from a different San Diego IP address in February 2008.

In addition, both the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report stated that the LabMD file was "detected being disclosed" in April 2008. Neither report indicated that Tiversa first downloaded the file from the San Diego IP address—an IP address not listed on either report—on February 5, 2008. Boback's deposition testimony and a cursory four-line document marked as exhibit CX-19 seem to be the only evidence that Tiversa first downloaded the LabMD file from a San Diego IP address in February 2008.

These documents contradict the information Tiversa provided to the FTC about the source and spread of the LabMD file. If Tiversa had, in fact, downloaded the LabMD file from the San Diego IP address and not from the Georgia IP address, then these reports should indicate as such. Instead, the San Diego IP address is nowhere to be found, and the Georgia IP address appears as the initial disclosing source on both reports.

Tiversa also produced an e-mail indicating that it originally downloaded the LabMD file from Georgia – and not from San Diego as it has steadfastly maintained to the FTC and this Committee. On September 5, 2013, Boback e-mailed Dan Kopchak and Molly Trunzo, both Tiversa employees, with a detailed summary of Tiversa's involvement with LabMD. Why Boback drafted the e-mail is unclear. He wrote, "[i]n 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name 'LabMD' in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located."¹⁹

As noted above, according to Alain Sheer, a senior FTC attorney assigned to the LabMD matter, the FTC did not narrow the September 2013 subpoena requiring Tiversa to produce, among other documents, "all documents related to LabMD."²⁰ Tiversa withheld these relevant

¹⁷ The IP address reported on the August 2008 forensic report that resolves to San Diego, California is 68.8.250.203. Boback testified, however, that Tiversa first downloaded the LabMD file from IP address 68.107.85.250 on February 5, 2008. Tiversa concluded in the report that the second IP address on which it observed the file was "most likely an IP shift from the original disclosing source."

¹⁸ *Id.*

¹⁹ E-mail from Robert Boback, CEO, Tiversa, to Dan Kopchak & Molly Trunzo (Sept. 5, 2013) (emphasis added) [TIVERSA-OGR-0028866-67].

²⁰ Tiversa FTC Subpoena.

documents about its discovery and early forensic analysis of the LabMD file from the FTC. These documents directly contradict testimony that Boback provided to the FTC, and call Tiversa's credibility into question. Boback has not adequately explained why his company withheld documents, and why his testimony is not consistent with reports Tiversa created at the time it discovered the LabMD file.

It is unlikely that the LabMD file analyzed in the April 2008 Incident Record Form and the August 2008 Forensic Investigative Report is different from the so-called "1718 file" at issue in the FTC proceeding, particularly given Boback's testimony to the FTC about how Tiversa's system names files.²¹ If, however, the earlier reports do refer to a different file, then Tiversa neglected to inform the FTC of a second, similarly sized leak of LabMD patient information.

Tiversa's June 2014 forensic report is the only report provided to this Committee that substantiates Boback's claims.

Tiversa produced to the Committee a forensic report on the LabMD file that it created in June 2014. Tiversa created this report and others related to testimony previously provided to the Committee after the investigation began. While outside the scope of the FTC's subpoena due to the date of the document, this is the only report supporting Tiversa's claim that it first downloaded the file from the San Diego IP address. This report contradicts information Tiversa provided to CIGNA in the April 2008 Incident Record Form and August 2008 Forensic Investigative Report—documents created much closer to when Tiversa purportedly discovered the LabMD document on a peer-to-peer network. The fact that Tiversa created the only forensic report substantiating its version of events after the Committee began its investigation raises serious questions.

This most recent report states that Tiversa's systems first detected the file on February 5, 2008, from a San Diego IP address (68.107.85.250) not included in either of the 2008 documents. According to the spread analysis, this San Diego IP shared the file from February 5, 2008, until September 20, 2011. Yet, despite allegedly being downloaded before both the April or August 2008 reports, neither 2008 document mentions that Tiversa downloaded this document.

The June 2014 report also states that the LabMD IP address (64.190.82.42) shared the file between March 7, 2007, and February 25, 2008. Thus, according to this report, by the time Tiversa submitted an Incident Record Form to CIGNA in April 2008, the LabMD IP address was no longer sharing the file. Furthermore, the report does not describe why Tiversa's system did not download the file from the Georgia IP address, even though the technology should have downloaded a file that hit on a search term, in this case "CIGNA," each time a different computer shared the document. The June 2014 report includes no reference to the other San Diego IP address discussed in the August 2008 forensic report as being in possession of the LabMD file.

²¹ Boback Nov. 2013 FTC Tr. at 40-41 (describing that a file's "hash" or title identifies "exactly what that file is." The title of the LabMD document described in the April and August 2008 documents is the same as the title of the document in the FTC proceeding).

Tiversa did not make a full and complete production of documents to this Committee. It is likely that Tiversa withheld additional documents from both this Committee and the FTC.

On October 14, 2014, Tiversa submitted a Notice of Information Pertinent to Richard Edward Wallace's Request for Immunity.²² Chief Administrative Law Judge D. Michael Chappell has since ordered that the assertions and documents contained in the Notice of Information will be "disregarded and will not be considered for any purpose."²³ Tiversa included two e-mails from 2012 as exhibits to the Notice of Information. According to Tiversa, these e-mails demonstrate that Wallace could not have fabricated the IP addresses in question in October 2013, because he previously included many of them in e-mails to himself and Boback a year prior.²⁴

Tiversa did not produce these documents to the Committee even though they are clearly responsive to the Committee's subpoena. Their inclusion in a submission in the FTC proceeding strongly suggests that Tiversa also never produced these documents to the FTC. In its Notice of Information, Tiversa did not explain how and when it identified these documents, why it did not produce them immediately upon discovery, and what additional documents it has withheld from both the FTC and the Committee. The e-mails also contain little substantive information and do not explain what exactly Wallace conveyed to Boback in November 2012 or why he conveyed it.

If Boback did in fact receive this information in November 2012, his June 2013 deposition testimony is questionable. It is surprising that Tiversa would have supplied inaccurate information to the FTC when Boback himself apparently received different information just months prior. Tiversa should have located and produced these e-mails pursuant to the September 2013 subpoena, and it should have been available for Boback's June 2013 deposition.

Tiversa's failure to produce numerous relevant documents to the Commission demonstrates a lack of good faith in the manner in which the company has responded to subpoenas from both the FTC and the Committee. It also calls into question Tiversa's credibility as a source of information for the FTC. The fact remains that withheld documents contemporaneous with Tiversa's discovery of the LabMD file directly contradict the testimony and documents Tiversa did provide. In the Committee's estimation, the FTC should no longer consider Tiversa to be a cooperating witness. Should the FTC request any further documents from Tiversa, the Commission should take all possible steps to ensure that Tiversa does not withhold additional documents relevant to the proceeding.

²² Tiversa Holding Corp.'s Notice of Information Pertinent to Richard Edward Wallace's Request For Immunity, In the Matter of Lab MD, Inc., No. 9357 (U.S. Fed. Trade Comm'n, Oct. 14, 2014), <http://www.ftc.gov/system/files/documents/cases/572572.pdf> [hereinafter Notice of Information].

²³ *LabMD Case: FTC gets green light to grant former Tiversa employee immunity in data security case*, PHIprivacy.net, Nov. 19, 2014, <http://www.phiprivacy.net/labmd-case-ftc-gets-green-light-to-grant-former-tiversa-employee-immunity-in-data-security-case/>.

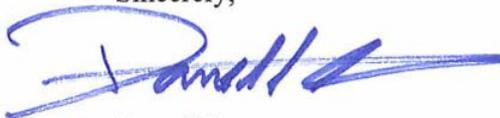
²⁴ Notice of Information at 4.

The Honorable Edith Ramirez
December 1, 2014
Page 8

I have enclosed the documents discussed herein with this letter, so that your staff may examine them. All documents are provided in the same form in which Tiversa produced them to the Committee.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X. If you have any questions, please contact the Committee staff at (202) 225-5074. Thank you for your prompt attention to this matter.

Sincerely,



Darrell Issa
Chairman

Enclosures

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Ms. Kelly Tshibaka, Acting Inspector General, U.S. Federal Trade Commission

Ms. Laura Riposo VanDruff, Complaint Counsel, U.S. Federal Trade Commission



INVESTIGATION REQUEST FORM

Section 1 Customer Information	
Organization Name	CIGNA
Contact Name	Sean Ryan
Contact Phone Number	(860) 226-7107
Contact Email Address	scan.ryan@cigna.com

Section 2 Incident Information	
Tiversa Incident Number	CIG00081
Date of Incident	4/18/2008

Section 3 Requested Forensic Services	
<p>File Disclosure Investigation</p> <p><input type="checkbox"/> 1. Disclosure Source Identification</p> <p><input type="checkbox"/> 2. Disclosure Source Geo-location</p> <p><input type="checkbox"/> 3. Identify Additional Disclosure Source Files</p> <p><input type="checkbox"/> 4. File Proliferation Assessment</p> <p><input type="checkbox"/> 5. Proliferation Point Identification</p> <p><input type="checkbox"/> 6. Proliferation Point Geo-location</p> <p><input type="checkbox"/> 7. Proliferation Point Associated Files</p>	<p>Search Investigation</p> <p><input type="checkbox"/> 12. Review Stored Searches For File Targeting</p> <p><input type="checkbox"/> 13. Track Searches for Specific File or Term</p>
<p>Persons of Interest (PoI)</p> <p><input type="checkbox"/> 8. Identify Persons of Interest</p> <p><input type="checkbox"/> 9. Track Specific Behavior of Persons of Interest</p> <p><input type="checkbox"/> 10. Identify Files Associated with Persons of Interest</p> <p><input type="checkbox"/> 11. Track Persons of Interest Download Behavior</p>	<p>Miscellaneous</p> <p><input type="checkbox"/> 14. Prosecution Support (Complete Section 4)</p> <p><input type="checkbox"/> 15. Other (Complete Section 4)</p>

Section 4 Specific Information Related to Request

TIVERSA – CUSTOMER RESTRICTED

Section 5 Additional Questions That Tiversa Can Address

More information can be gathered related to this disclosure by leveraging Tiversa's P2P File Sharing Forensic Investigation Services. If requested, please fill out the Investigation Request form located below and submit to your Account Manager.

Who is the individual disclosing the information?

Select investigation services #1 and #3

What else is this individual sharing or disclosing?

Select investigation service #3

Where is this individual located in the world?

Select investigation service #2

Did the files spread to other users of the network?

Select investigation services #4

TIVERSA – CUSTOMER RESTRICTED



Forensic Investigation Report for Ticket #CIG00081

August 12, 2008

CONFIDENTIAL

2.1 File Proliferation Analysis

The CIGNA-related file identified in Ticket #81, as well as some of the files not related to CIGNA, have been observed by Tiversa at additional IP addresses on the P2P. However, network constraints and/or user behavior prevented Tiversa from downloading the files from these additional sources. Most likely, the user logged off the P2P prior to or while Tiversa was attempting to acquire the files.

Regardless, information regarding these new observations is included in Figure 2-1-1 immediately below.

**Figure 2-1-1:
File Proliferation Details**

Proliferation Point	File Title	IP Address	Date Observed	IP Geo-Location	ISP	Source
0	insuranceaging_6.05.071.pdf	64.190.82.42	4/18/08	Atlanta, GA	Cypress Communications	Original Source from Ticket #81
1	insuranceaging_6.05.071.pdf	64.190.79.36	8/1/08	Oakwood, GA	Cypress Communications	Probably an IP shift of original source
2	insuranceaging_6.05.071.pdf	68.8.250.203	8/5/08	San Diego, CA	Cox Communications	Unknown (based on other files observed, possible Information Concentrator)

Based on the other files available at the new IP addresses, Proliferation Point #1 (from Figure 2-1-1 above) is most likely an IP shift from the original disclosing source identified in Ticket #81. However, the other files present at Proliferation Point #2 suggest that this source could be an Information Concentrator. Because Tiversa analysts were only able to visually observe these new sources, rather than actually download files, further data collection and analysis may be required for full source identification of the proliferation points.

2.2 Additional Data Collection/ Analysis

Tiversa is currently attempting to re-acquire these sources and download any relevant files from them.

3. Conclusions/ Suggested Actions

It appears evident that the files from Ticket #81 have proliferated across the P2P and are available from additional IP addresses. However, clear identification of these new sources is not conclusive at this time. Tiversa will update this report as new information becomes available.



2000 Corporate Drive, Suite 300
Wexford, Pennsylvania 15090

724 940-9030
724 940-9033

www.tiversa.com

From: Robert Boback <rboback@tiversa.com>
Sent: Thursday, September 5, 2013 3:20 PM
To: Dan Kopchak <dkopchak@tiversa.com>; Molly Trunzo <mtrunzo@tiversa.com>
Subject: Tiversa

I wanted to provide updated information regarding the question of litigation involving Tiversa. During our call, I discussed litigation in which Tiversa is a plaintiff against our former patent firm. That is still ongoing. Earlier in 2013, Tiversa was also engaged in a separate litigation with a company called LabMD, which is based in Georgia. Tiversa, Dartmouth College and Professor Eric Johnson (Tuck Business School) was sued by LabMD by its CEO, Michael Daugherty as he alleged that Tiversa "hacked" his company in an effort to get a file containing nearly 9,000 patient's SSNs and medical information and provided the information to Dartmouth and Eric Johnson for a DHS-funded research project. Mr. Daugherty has little to no understanding of P2P or information security which is what caused him to think that he was "hacked" and which resulted in his widespread government conspiracy theory that followed. He also suggested in the litigation that because he would not do business with Tiversa to remediate the problem, that Tiversa "kicked the file over to the feds [FTC]" (and Dartmouth) and the FTC sent him a questionnaire about the breach, which caused him "great harm" due to the widespread "government shakedown of small business." He claimed that Tiversa was attempting to extort money from him to "answer his questions" as a part of the larger conspiracy. The reason that I did not mention this during our discussion is that the case was dismissed due to jurisdiction (his real estate attorney friend filed it in Georgia). He subsequently appealed two times, and lost both, the final of which was ruled on in February 2013. As an interesting sidebar to this story, Mr. Daugherty began writing a book about the government overreach and his great conspiracy theory of the government war on small business. When our attorneys learned of what was coming in the book (from his blog postings about the book), we quickly served his counsel with a C&D as his "true story" was full of inaccurate statements about me and Tiversa. Unfortunately, Mr. Daugherty sees himself as "Batman" (no joke) and he chose to continue on with his book and starting scheduling speaking engagements where he would discuss his "true story" about how the government is out to "get" small business and that the FTC and Tiversa (and presumably Dartmouth) are the ring leaders. His book, "Devil inside the Beltway" is to be released later this month. While I do not expect this book to be on the NY Times best seller list, I cannot sit idly by and allow such a gross distortion of the facts and mischaracterization of Tiversa, and me, in his efforts to sell his book and create a "name" for himself on any speaking tour.

That said, Tiversa filed a complaint in federal court today citing a number of counts including but not limited to Defamation, Slander, Libel, and others against Mr. Daugherty and LabMD. Tiversa is not litigious and it was our hope that he would conduct himself appropriately after receiving the C&D in November of 2012. But again, he sees himself as Batman.

Here is the real series of events that occurred in this case:

Tiversa, as you know, downloads leaked information on behalf of clients, individual, corporate and/or federal. In the process of downloading information, we often get files that are not related to our clients but are nonetheless sensitive. We call this "dolphin in the tuna net"....for example, if we were looking for "Goldman Sachs" and our system finds a file with the term "Goldman" in it. The file may have the name "Henry Goldman" but our system just saw "Goldman" and downloaded it, in the event it related to Goldman Sachs. After the file would be downloaded, it would be reviewed by an Analyst which would determine that it was NOT related to Goldman Sachs, but it may or may not include SSNs or other sensitive information. This was the case with LabMD.

In 2008, while doing work for a client, our systems downloaded a file (1,718 page pdf) that contained sensitive information including SSNs and health information for over 9000 people. The file had the name "LabMD" in both the header of the file and the metadata. The IP of the download was found to be in Georgia, which after a Google search, is where we found LabMD's office to be located. At this point, we were not positive that the file belonged to LabMD, but it seemed probable. We could have chosen to do nothing at all and pretend that we never saw the file. That approach would leave both LabMD and the 9000 victims at very high risk (and growing) of fraud and identity theft. Needless to say, we contacted the company to inform them of the file with their company name on it. After providing the file with all of the information that we had, the Mr. Daugherty asked us for additional information that we did not have. We told him that we could perform the services but it would take a few weeks and would cost about \$15K. After hearing this, he asked us to send him the SOW for the services. 28 weeks after providing the SOW and not hearing anything in return, I reached out to Mr. Daugherty to see if he had any questions (re: SOW) and he told me never to contact him again with no further explanation. We didn't.

Tuck Business School at Dartmouth (and Professor Eric Johnson) used Tiversa in early 2006 for a research project to determine to what extent, if any, leaked financial documents were able to be found on P2P networks. The research consisted of Dartmouth providing simple and straightforward search terms to Tiversa like "bank" and "account" to locate and download files using Tiversa's engine to a hard drive that Dartmouth owned and controlled. Tiversa only issued the searches but was not able to see the actual downloads. The downloads were stored on a hard drive that graduate students at Dartmouth were to later evaluate. Although Dartmouth was researching this using resources from a grant by DHS, Tiversa was not paid anything for our participation. The research was impactful and resulted in a number of articles being published. With the prior success of the financial research, Dartmouth wanted to followup with a second research project focused on medical information in 2008. Following the exact same procedure, the medical research was completed and widely published in early 2009. Again, Tiversa did not receive any compensation whatsoever for our part in the project. Upon reading the research paper, one of the many example files that were used to demonstrate the problem was the file in question with LabMD. Tiversa did not know that the file was included in the research as we did not see the downloads, only the search terms. Frankly, it was not surprising that the file was found because it was never addressed with LabMD therefore the file continued to spread across the P2P network.

I was called to testify before Congress twice in 2009, once in May and the second in July, as they were investigating breaches of security via P2P. At the director Congress, Tiversa was asked to demonstrate the extent and severity of the problem. Tiversa then provided Congress with numerous, redacted, examples of file disclosure that affected government, private and public enterprises, and individuals. Shortly after the hearings, Tiversa was visited by the FTC. The senior representatives from the FTC wanted to see the non-redacted versions of the files discussed with Congress as one of their missions is to help consumers handle ID theft. When Tiversa asked what would happen if we refused to provide the information, the FTC stated that they would issue a Civil Investigative Demand (CID which acts as a federal subpoena to gain access to the information. We told them that they would need to do that and then we would provide the information in accordance with the subpoena. The FTC issued a subpoena that asked us to provide any file, regardless of source, that disclosed >100 SSNs. We provided over 100 files to the FTC in accordance with the federal subpoena and the LabMD file was still one of them as it remained on the P2P network. We had no insight/control as to what the FTC was going to do with the information once they received it. Tiversa was not compensated in any way for providing this information to the FTC.

Apparently, the FTC sent questionnaires to some, if not all, of the companies or organizations that breached the sensitive information. The FTC posted on its website a copy of a standard letter(s) that was sent, which is how we knew that they had sent a letter or letters. We had no further communication with the FTC regarding the breaches or their investigations.

LabMD sued Tiversa/Dartmouth/Eric Johnson. Case was dismissed (all three times) for jurisdiction issues.



Forensic Investigation Report - LABMD0001

Prepared for LabMD

SECTION 1 - Customer Information

Organization Name	N/A
Contact Name	N/A
Contact Phone	N/A
Contact Email	N/A

SECTION 2 - Incident Information

Incident Number	LABMD0001
Related Incidents	N/A
Date of Report	6/4/2014
Severity	URGENT

SECTION 3 - Preliminary Disclosure Information

IP Address	64.190.82.42
P2P Client	N/A
Disclosure Type	Internal
Disclosure Source	LabMD
Filename(s)	insuranceaging_6.05.071.pdf

SECTION 4 - Incident Summary

On 2/5/2008, Tiversa's systems detected 1 file being disclosed on P2P file sharing networks. The detected file appears to be a 1,718 page "Insurance Aging" Report relating to "LABMD, INCORPORATED." The file contains patient information including Name, Social Security Number, DOB, Insurance Information, Billing Date Code/CPT, Billed Amount etc., relating to approximately 9,000 apparent patients.

The file appears to be emanating from the IP Address 64.190.82.42, which traces to Atlanta, Georgia, US.

Upon further analysis, 19 total files were detected being disclosed from this IP address on various dates between 3/7/2007 and 2/25/2008. The additional files include Insurance Benefits labels, LabMD login credentials (username and passwords) relating to web access for insurance companies, LabMD Insurance Verification Specialist Duties, blank forms relating to daily credit card transactions, LabMD Medical Records Request letters, LabMD Patient Appeal Authorization letters, LabMD Payment Posting Specialist Duties, a LabMD Employee Handbook, LabMD Employee Time Off Request forms, documents containing meeting notes and other related letters.

Upon reviewing the metadata and files emanating from this source, Tiversa believes the disclosure source may be an individual employed with LabMD.

Figure 2-1-2:
Disclosure Source IP Address - 64.190.82.42

File Title	Disclosure Date	Company	Author	Last Saved by
INSURANCE BENEFITS LABELS.doc	3/7/2007		Liz Fair	sbrown
WEB ACCESS FOR INSURANCE COMPANIES.doc	3/7/2007	LabMD		sbrown
LabMD Insurance Verification Specialist Duties.doc	3/7/2007		sbrown	sbrown
HELPFUL TIPS FOR BETTER AUDIT RESULTS.doc	3/15/2007		sbrown	sbrown
DAILY CREDIT CARD TRANSACTIONS.doc	10/11/2007		sbrown	sbrown
MEDICAL RECORDS FEE LTR.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS RELEASE.doc	11/10/2007	labmd	Administrator	sbrown
MEDICAL RECORDS REQ LTR.doc	11/10/2007	labmd	Administrator	rwoodson
PATIENT APPEAL AUTHORIZATION LTR.doc	11/10/2007	labmd	Administrator	rwoodson
LabMD Payment Posting Specialist Duties.doc	11/10/2007		sbrown	rwoodson
Patient Locator Project.doc	11/13/2007		rwoodson	rwoodson
Humana patient Doc.doc	11/13/2007	labmd	rwoodson	rwoodson
Employee Handbbook.doc	11/15/2007		Dan Carmichael	
Employee Application Benefits.pdf	11/15/2007		a498584	
Employee Time Off Requests2007.doc	11/29/2007		rwoodson	rwoodson
insuranceaging_6.05.071.pdf	2/5/2008			
BCBS HMO & POS APPEAL LTR.doc	2/25/2008	labmd	Administrator	rwoodson
BCBS PAID PT LTR.doc	2/25/2008	labmd	Administrator	rwoodson
Rozs Coverage.doc	2/25/2008		rwoodson	rwoodson

One file emanating from this source appears to be a letter from the following individual:

Rosalind Woodson
Billing Manager/LabMD
rwoodson@labmd.org

This individual appears to be employed with LabMD and may have utilized the "rwoodson" user identifier as referenced within the metadata of the disclosed documents.

Figure 2-1-5:

WEB ACCESS FOR INSURANCE COMPANIES

BCBS FL (Not Available)

BCBS GA (www.bcbsga.com)
USER NAME: [REDACTED] PASSWORD: [REDACTED]

BCBS SC (www.southcarolinablues.com)
USER NAME: [REDACTED] PASSWORD: [REDACTED]

BCBS TN (www.bcbst.com)
USER NAME: [REDACTED] PASSWORD: [REDACTED]

HUMANA (www.humana.com)
USER NAME: [REDACTED] PASSWORD: [REDACTED]

Author:	LabMD
Manager:	
Company:	

Last saved by: sbrown
Revision number: 4
Total editing time: 20 Minutes

Figure 2-1-7:

LabMD Payment Posting Specialist Duties

INSURANCE PAYMENT POSTING

1. Posting Specialist will post insurance payments (correlate with Explanation of Benefits, including "no-pay" denials) from daily batches in [REDACTED]
2. After each insurance batch is posted, Posting Specialist will run "Day Sheet-Transaction Detail Report" to make sure payments posted in [REDACTED] "balance"/equals insurance deposit tape total.
 - a. Select "Reports" from Toolbar at Main Menu in [REDACTED]
 - b. Select "Day Sheet".
 - c. Under Options Tab, unclick "Subtotal by Provider" and
 - d. Select "Sort by Name".

Author: sbrown

Manager:

Company:

Last saved by: rwoodson

Revision number: 3

Total editing time: 34 Minutes

Figure 2-1-9:

LabMD
THE LABORATORY SERVICES COMPANY
1117 Perimeter Center West, Suite #1W-406, Atlanta, GA 30338 * (678) 443-2330/(888) 967-8743 * Fax (678) 443-2329

March 23, 2007

To Whom It May Concern:

This letter serves as a formal request to have claims for the attached list of patients reprocessed

If you have any further questions, do not hesitate to contact me directly at (678) 443-2338, Monday through Friday, between 8am - 6pm.

Sincerely,

Rosalind Woodson
Billing Manager/LabMD
rwoodson@labmd.org

Author:	Administrator
Manager:	
Company:	labmd

Last saved by:	rwoodson
Revision number:	6
Total editing time:	20 Minutes

3. Conclusions/Suggested Actions

In order to contain any further proliferation of these LabMD-related files across the P2P networks, any computers responsible for their disclosure must be identified and then removed from the P2P networks – or at a minimum, the LabMD related files must be removed from the suspect's machine.

Based on the information reviewed by Tiversa, a suggested course of action is to contact the apparent LabMD employees listed within the Investigation findings above (Rosalind Woodson and Sandra Brown) reference the disclosed document titles, document content, and the supporting evidence listed above. It is possible that an investigation into these disclosed files and possible sources will allow LabMD to determine the disclosure source. If the disclosure source machine is found, the machine should be reviewed for the presence of file sharing software. An investigation of this machine should indicate that the files found on that machine match the file listing noted in Figure 2-1-2 above. It should be noted that the disclosure source machine may be a home computer, work computer or possibly a laptop.

Additional remediation activities can be discussed with Tiversa once additional investigation steps by LabMD have been completed.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

February 20, 2015

The Honorable Richard Blumenthal
United States Senate
Washington, DC 20510

Dear Senator Blumenthal:

Thank you for your letter of February 6, requesting that the Federal Trade Commission (“Commission” or “FTC”) investigate Verizon’s disclosures regarding its use of mobile tracking technologies, including so-called “supercookies.” I appreciate your strong support for consumer privacy, and I share your concerns about the use of persistent identifiers to regenerate browser cookies that consumers previously deleted from their mobile devices.

Commission staff is reviewing your letter and the attached privacy policy. I can assure you that your request and the concerns you have expressed are receiving careful consideration. As you know, Commission investigations are non-public, and I cannot comment on any specific current or possible future investigations.

The Commission has authority to take action against practices that are deceptive or unfair under Section 5 of the FTC Act, 15 U.S.C. § 45. A representation, omission, or practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances, and (2) it is material, that is, likely to affect consumers’ conduct or decisions regarding the product at issue.¹ An act or practice is unfair if the injury it causes or is likely to cause to consumers (1) is substantial; (2) is not outweighed by countervailing benefits to consumers or to competition; and (3) is not reasonably avoidable by consumers themselves.²

I cannot comment specifically on whether the particular practices you reference would violate Section 5 of the FTC Act. Generally, however, in determining whether to take action in any particular situation, the Commission may consider a number of factors. For example, the Commission could take action if a company misrepresents the extent to which consumers’ data is collected, used, shared, or disclosed. For example, in November 2011, the Commission settled charges with advertising network ScanScout, Inc.³ The Commission charged ScanScout with

¹ *Kraft, Inc.*, 114 F.T.C. 40, 120 (1991), *aff’d*, 970 F.2d 311 (7th Cir. 1992), *cert. denied*, 507 U.S. 909 (1993); *see generally, Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs.*, 103 F.T.C. 110, 174-83 (1984).

² Section 5(n) of the FTC Act, 15 U.S.C. 45(n), *added by The Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-112*.

³ *In re ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (final consent order), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>. *See also In re Epic Marketplace, Inc.*, FTC Docket No. C-4389 (Mar. 13, 2013) (final consent order) (settling charges that Epic

engaging in deceptive practices by claiming that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies. According to the Commission's complaint, however, ScanScout used Flash cookies, which browser settings could not block. The Commission's order requires, among other things, that ScanScout accurately describe its data practices, provide consumers with an effective opt-out mechanism and provide a homepage disclosure with a direct link to the opt-out mechanism, as well as enhanced notice within targeted ads displayed to consumers.

The Commission is continuing its work to protect consumers' privacy online, through its enforcement activities, outreach to consumers and industry, and monitoring of the marketplace. The FTC provides guidance to businesses and consumers through materials that can be found on our website. For example, the FTC has issued consumer guidance describing what cookies are, how they operate, and providing tips to help consumers control their use.⁴ And, I believe that disclosures and choices provided to consumers should apply to all technologies, or consumers who believe they are making choices about tracking may be deceived.⁵ In short, companies should not make statements about choices available to consumers, and then circumvent those choices using different technologies.

Finally, as you know, the Federal Communications Commission ("FCC") is considering whether to reclassify consumer broadband services. I share the goal of ensuring an open Internet and respect the FCC's efforts to address this important and complex issue. However, I want to note that reclassification of consumer broadband services may divest the FTC of some of its jurisdiction, likely including the practices at issue in your letter. I think it is important that the FTC, with its decades of experience in consumer protection, continue to contribute to the protection of consumers who purchase broadband services. For this reason, the Commission, on a bipartisan basis, has long supported the repeal of the outdated provision in the FTC Act that prevents the agency from addressing common carrier services.

If you or your staff have additional questions on these matters or wish to share additional information with us, please do not hesitate to contact me or have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at 202-326-2946.

Sincerely,



Edith Ramirez
Chairwoman

Marketplace, Inc. used browser "history sniffing" to secretly and illegally determine whether millions of consumers had visited any of more than 54,000 domains), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc>.

⁴ "Cookies: Leaving a Trail on the Web," FEDERAL TRADE COMMISSION (Nov. 2011), <http://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web>.

⁵ *See, e.g.*, Remarks of Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission, *Beyond Cookies: Privacy Lessons for Online Advertising*, AdExchanger Industry Preview at 9 (Jan. 21, 2015), *available at* <http://www.ftc.gov/public-statements/2015/01/beyond-cookies-privacy-lessons-online-advertising-adexchanger-industry>.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

February 20, 2015

The Honorable Edward J. Markey
United States Senate
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter of February 6, requesting that the Federal Trade Commission (“Commission” or “FTC”) investigate Verizon’s disclosures regarding its use of mobile tracking technologies, including so-called “supercookies.” I appreciate your strong support for consumer privacy, and I share your concerns about the use of persistent identifiers to regenerate browser cookies that consumers previously deleted from their mobile devices.

Commission staff is reviewing your letter and the attached privacy policy. I can assure you that your request and the concerns you have expressed are receiving careful consideration. As you know, Commission investigations are non-public, and I cannot comment on any specific current or possible future investigations.

The Commission has authority to take action against practices that are deceptive or unfair under Section 5 of the FTC Act, 15 U.S.C. § 45. A representation, omission, or practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances, and (2) it is material, that is, likely to affect consumers’ conduct or decisions regarding the product at issue.¹ An act or practice is unfair if the injury it causes or is likely to cause to consumers (1) is substantial; (2) is not outweighed by countervailing benefits to consumers or to competition; and (3) is not reasonably avoidable by consumers themselves.²

I cannot comment specifically on whether the particular practices you reference would violate Section 5 of the FTC Act. Generally, however, in determining whether to take action in any particular situation, the Commission may consider a number of factors. For example, the Commission could take action if a company misrepresents the extent to which consumers’ data is collected, used, shared, or disclosed. For example, in November 2011, the Commission settled charges with advertising network ScanScout, Inc.³ The Commission charged ScanScout with

¹ *Kraft, Inc.*, 114 F.T.C. 40, 120 (1991), *aff’d*, 970 F.2d 311 (7th Cir. 1992), *cert. denied*, 507 U.S. 909 (1993); *see generally, Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs.*, 103 F.T.C. 110, 174-83 (1984).

² Section 5(n) of the FTC Act, 15 U.S.C. 45(n), *added by The Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-112*.

³ *In re ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (final consent order), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>. *See also In re Epic Marketplace, Inc.*, FTC Docket No. C-4389 (Mar. 13, 2013) (final consent order) (settling charges that Epic

engaging in deceptive practices by claiming that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies. According to the Commission's complaint, however, ScanScout used Flash cookies, which browser settings could not block. The Commission's order requires, among other things, that ScanScout accurately describe its data practices, provide consumers with an effective opt-out mechanism and provide a homepage disclosure with a direct link to the opt-out mechanism, as well as enhanced notice within targeted ads displayed to consumers.

The Commission is continuing its work to protect consumers' privacy online, through its enforcement activities, outreach to consumers and industry, and monitoring of the marketplace. The FTC provides guidance to businesses and consumers through materials that can be found on our website. For example, the FTC has issued consumer guidance describing what cookies are, how they operate, and providing tips to help consumers control their use.⁴ And, I believe that disclosures and choices provided to consumers should apply to all technologies, or consumers who believe they are making choices about tracking may be deceived.⁵ In short, companies should not make statements about choices available to consumers, and then circumvent those choices using different technologies.

Finally, as you know, the Federal Communications Commission ("FCC") is considering whether to reclassify consumer broadband services. I share the goal of ensuring an open Internet and respect the FCC's efforts to address this important and complex issue. However, I want to note that reclassification of consumer broadband services may divest the FTC of some of its jurisdiction, likely including the practices at issue in your letter. I think it is important that the FTC, with its decades of experience in consumer protection, continue to contribute to the protection of consumers who purchase broadband services. For this reason, the Commission, on a bipartisan basis, has long supported the repeal of the outdated provision in the FTC Act that prevents the agency from addressing common carrier services.

If you or your staff have additional questions on these matters or wish to share additional information with us, please do not hesitate to contact me or have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at 202-326-2946.

Sincerely,



Edith Ramirez
Chairwoman

Marketplace, Inc. used browser "history sniffing" to secretly and illegally determine whether millions of consumers had visited any of more than 54,000 domains), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc>.

⁴ "Cookies: Leaving a Trail on the Web," FEDERAL TRADE COMMISSION (Nov. 2011), <http://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web>.

⁵ See, e.g., Remarks of Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission, *Beyond Cookies: Privacy Lessons for Online Advertising*, AdExchanger Industry Preview at 9 (Jan. 21, 2015), available at <http://www.ftc.gov/public-statements/2015/01/beyond-cookies-privacy-lessons-online-advertising-adexchanger-industry>.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

February 20, 2015

The Honorable Bill Nelson
United States Senate
Washington, DC 20510

Dear Senator Nelson:

Thank you for your letter of February 6, requesting that the Federal Trade Commission (“Commission” or “FTC”) investigate Verizon’s disclosures regarding its use of mobile tracking technologies, including so-called “supercookies.” I appreciate your strong support for consumer privacy, and I share your concerns about the use of persistent identifiers to regenerate browser cookies that consumers previously deleted from their mobile devices.

Commission staff is reviewing your letter and the attached privacy policy. I can assure you that your request and the concerns you have expressed are receiving careful consideration. As you know, Commission investigations are non-public, and I cannot comment on any specific current or possible future investigations.

The Commission has authority to take action against practices that are deceptive or unfair under Section 5 of the FTC Act, 15 U.S.C. § 45. A representation, omission, or practice is deceptive if (1) it is likely to mislead consumers acting reasonably under the circumstances, and (2) it is material, that is, likely to affect consumers’ conduct or decisions regarding the product at issue.¹ An act or practice is unfair if the injury it causes or is likely to cause to consumers (1) is substantial; (2) is not outweighed by countervailing benefits to consumers or to competition; and (3) is not reasonably avoidable by consumers themselves.²

I cannot comment specifically on whether the particular practices you reference would violate Section 5 of the FTC Act. Generally, however, in determining whether to take action in any particular situation, the Commission may consider a number of factors. For example, the Commission could take action if a company misrepresents the extent to which consumers’ data is collected, used, shared, or disclosed. For example, in November 2011, the Commission settled charges with advertising network ScanScout, Inc.³ The Commission charged ScanScout with

¹ *Kraft, Inc.*, 114 F.T.C. 40, 120 (1991), *aff’d*, 970 F.2d 311 (7th Cir. 1992), *cert. denied*, 507 U.S. 909 (1993); *see generally*, *Federal Trade Commission Policy Statement on Deception, appended to Cliffdale Assocs.*, 103 F.T.C. 110, 174-83 (1984).

² Section 5(n) of the FTC Act, 15 U.S.C. 45(n), *added by The Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-112.*

³ *In re ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (final consent order), *available at* <http://www.ftc.gov/enforcement/cases-proceedings/102-3185/scanscout-inc-matter>. *See also In re Epic Marketplace, Inc.*, FTC Docket No. C-4389 (Mar. 13, 2013) (final consent order) (settling charges that Epic

engaging in deceptive practices by claiming that consumers could opt out of receiving targeted ads by changing their computer's web browser settings to block cookies. According to the Commission's complaint, however, ScanScout used Flash cookies, which browser settings could not block. The Commission's order requires, among other things, that ScanScout accurately describe its data practices, provide consumers with an effective opt-out mechanism and provide a homepage disclosure with a direct link to the opt-out mechanism, as well as enhanced notice within targeted ads displayed to consumers.

The Commission is continuing its work to protect consumers' privacy online, through its enforcement activities, outreach to consumers and industry, and monitoring of the marketplace. The FTC provides guidance to businesses and consumers through materials that can be found on our website. For example, the FTC has issued consumer guidance describing what cookies are, how they operate, and providing tips to help consumers control their use.⁴ And, I believe that disclosures and choices provided to consumers should apply to all technologies, or consumers who believe they are making choices about tracking may be deceived.⁵ In short, companies should not make statements about choices available to consumers, and then circumvent those choices using different technologies.

Finally, as you know, the Federal Communications Commission ("FCC") is considering whether to reclassify consumer broadband services. I share the goal of ensuring an open Internet and respect the FCC's efforts to address this important and complex issue. However, I want to note that reclassification of consumer broadband services may divest the FTC of some of its jurisdiction, likely including the practices at issue in your letter. I think it is important that the FTC, with its decades of experience in consumer protection, continue to contribute to the protection of consumers who purchase broadband services. For this reason, the Commission, on a bipartisan basis, has long supported the repeal of the outdated provision in the FTC Act that prevents the agency from addressing common carrier services.

If you or your staff have additional questions on these matters or wish to share additional information with us, please do not hesitate to contact me or have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at 202-326-2946.

Sincerely,



Edith Ramirez
Chairwoman

Marketplace, Inc. used browser "history sniffing" to secretly and illegally determine whether millions of consumers had visited any of more than 54,000 domains), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3182/epic-marketplace-inc>.

⁴ "Cookies: Leaving a Trail on the Web," FEDERAL TRADE COMMISSION (Nov. 2011), <http://www.consumer.ftc.gov/articles/0042-cookies-leaving-trail-web>.

⁵ See, e.g., Remarks of Jessica Rich, Director, Bureau of Consumer Protection, Federal Trade Commission, *Beyond Cookies: Privacy Lessons for Online Advertising*, AdExchanger Industry Preview at 9 (Jan. 21, 2015), available at <http://www.ftc.gov/public-statements/2015/01/beyond-cookies-privacy-lessons-online-advertising-adexchanger-industry>.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

March 03, 2015

The Honorable Charles J. Fleischmann
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Fleischmann:

Thank you for your January 27, 2015 letter concerning recent price increases for many generic prescription drugs. You ask the FTC to carefully examine such pricing activity and request information that may shed further light on this topic. We appreciate your interest and vigilance in this critically important area.

Protecting American consumers from anticompetitive mergers and practices in the health care sector has long been one of our most important responsibilities. I can therefore assure you that we will continue to use our statutory authority to protect health care consumers whenever appropriate. As a general matter, of course, Congress has empowered the Commission to prevent unfair methods of competition that violate Section 5 of the Federal Trade Commission Act,¹ such as illegally anticompetitive agreements among competitors to increase prices or restrict output, and illegally exclusionary or predatory practices. Congress also has empowered the Commission to prevent mergers, acquisitions, and certain other practices that may substantially lessen competition or tend to create a monopoly, in violation of the Clayton Act.²

The agency's recent antitrust enforcement actions, reports, and other activities involving generic drugs are available on the Commission's website.³ We are aware of recent reports of significant price increases for at least some generic drugs and will continue to monitor the marketplace in an effort to understand the factors at play. I should note that, to the extent that prescription drug price increases are linked to shortages of supply caused by market factors, the U.S. Food and Drug Administration can be expected to exercise its legal authority to address and

¹ 15 U.S.C. § 45. Section 5 of the FTC Act prohibits, among other conduct, practices that violate the Sherman Act, including in particular monopolization, attempts to monopolize, conspiracies to monopolize, and conspiracies in restraint of trade. *See generally* *FTC v. Cement Inst.*, 333 U.S. 683, 690 (1948).

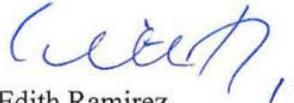
² 15 U.S.C. §§ 12 *et seq.*

³ The Commission has placed an overview of its actions and activities involving pharmaceutical and other health care markets at <http://www.ftc.gov/tips-advice/competition-guidance/industry-guidance/health-care>.

prevent such shortages.⁴ We have therefore taken the liberty of forwarding your letter to the FDA for consideration under that agency's jurisdiction as well.

Thank you again for raising this topic. Protecting consumers from anticompetitive activity in the pharmaceutical industry remains a top priority for the Commission. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,



Edith Ramirez
Chairwoman

cc: The Honorable Margaret A. Hamburg, M.D.
Commissioner of Food and Drugs
U.S. Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

⁴ <http://www.fda.gov/Drugs/drugsafety/DrugShortages/default.htm>.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

October 28, 2014

The Honorable Amy Klobuchar
United States Senate
Washington, D.C. 20510

Dear Senator Klobuchar:

Thank you for the October 17, 2014 letter from you and Senator Lee regarding the proposed merger of US Foods, Inc. and Sysco Corporation. We appreciate receiving the information and views presented in your correspondence.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the disclosure of the contours of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction. I can assure you that the Commission is committed to conducting a thorough investigation, and to considering all pertinent information and views gathered, as we do in all our investigations. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you again for bringing your observations to our attention in this important matter. As always, we appreciate your interest and vigilance in maintaining competition and protecting consumers in the marketplace. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

October 28, 2014

The Honorable Mike Lee
United States Senate
Washington, D.C. 20510

Dear Senator Lee:

Thank you for the October 17, 2014 letter from you and Senator Klobuchar regarding the proposed merger of US Foods, Inc. and Sysco Corporation. We appreciate receiving the information and views presented in your correspondence.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the disclosure of the contours of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction. I can assure you that the Commission is committed to conducting a thorough investigation, and to considering all pertinent information and views gathered, as we do in all our investigations. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you again for bringing your observations to our attention in this important matter. As always, we appreciate your interest and vigilance in maintaining competition and protecting consumers in the marketplace. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

November 25, 2014

The Honorable Charles Grassley
United States Senate
Washington, D.C. 20510

Dear Senator Grassley:

Thank you for the October 29, 2014 letter from you and Senator Klobuchar regarding the release of Commission staff reports that provide information on the agreements between branded and generic pharmaceutical companies filed with the Federal Trade Commission and Department of Justice pursuant to the requirements of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 ("MMA"). We share your appreciation that these annual staff reports should be prepared and released expeditiously. We also recognize that they provide important information to help illuminate the continued anticompetitive impact of pay-for-delay agreements on consumers, particularly in light of the U.S. Supreme Court's ruling last year in *FTC v. Actavis Inc.* clarifying that these agreements are subject to antitrust scrutiny.

FTC staff continues to work diligently to review and categorize agreements received under the MMA and expect to issue the 2013 fiscal year report by the end of this year. We intend to issue the report on the 2014 fiscal year, which ended in September, as soon as possible thereafter. Preparing these reports is a time-intensive endeavor, requiring legal analysis and the categorization of a large number of complex and lengthy agreements. In fiscal year 2013, we received over 180 agreements; we received approximately 200 agreements in FY 2014. Our review of the competitive implications of these agreements also includes consideration of certain non-public information that we receive from the Food and Drug Administration. Finally, to ensure consistency and accuracy on this important project, we subject our staff reports to various levels of management review.

Protecting consumers from anticompetitive agreements in the pharmaceutical industry remains a top priority for the Commission. Thank you again for raising this topic with me, and please let me know if we can be of further service in this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Edith Ramirez".

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

November 25, 2014

The Honorable Amy Klobuchar
United States Senate
Washington, D.C. 20510

Dear Senator Klobuchar:

Thank you for the October 29, 2014 letter from you and Senator Grassley regarding the release of Commission staff reports that provide information on the agreements between branded and generic pharmaceutical companies filed with the Federal Trade Commission and Department of Justice pursuant to the requirements of the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 ("MMA"). We share your appreciation that these annual staff reports should be prepared and released expeditiously. We also recognize that they provide important information to help illuminate the continued anticompetitive impact of pay-for-delay agreements on consumers, particularly in light of the U.S. Supreme Court's ruling last year in *FTC v. Actavis Inc.* clarifying that these agreements are subject to antitrust scrutiny.

FTC staff continues to work diligently to review and categorize agreements received under the MMA and expect to issue the 2013 fiscal year report by the end of this year. We intend to issue the report on the 2014 fiscal year, which ended in September, as soon as possible thereafter. Preparing these reports is a time-intensive endeavor, requiring legal analysis and the categorization of a large number of complex and lengthy agreements. In fiscal year 2013, we received over 180 agreements; we received approximately 200 agreements in FY 2014. Our review of the competitive implications of these agreements also includes consideration of certain non-public information that we receive from the Food and Drug Administration. Finally, to ensure consistency and accuracy on this important project, we subject our staff reports to various levels of management review.

Protecting consumers from anticompetitive agreements in the pharmaceutical industry remains a top priority for the Commission. Thank you again for raising this topic with me, and please let me know if we can be of further service in this or any other matter.

Sincerely,

A handwritten signature in blue ink, appearing to read "Edith Ramirez".

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 8, 2014

The Honorable Martin Heinrich
United States Senate
Washington, D.C. 20510

Dear Senator Heinrich:

Thank you for the November 12, 2014 letter from you and Senator Udall requesting that the Commission give due consideration to concerns that New Mexico-based Plant Oil Powered Diesel Fuel Systems, Inc. ("POP Diesel") recently raised with the FTC about certain standard-setting decisions by ASTM International that it believes may be impeding competition.

You report that POP Diesel produces equipment that enables any diesel engine to run on 100 percent vegetable oil fuel, and that the company is aiming to establish a nationwide network of filling stations devoted to this fuel following the Environmental Protection Agency's approval last year of the use of such fuel with POP Diesel's technology. You also mention that state and federal authorities often incorporate ASTM's standards into legal requirements, and that the exclusion of pure plant oil from ASTM fuel standards could thus harm the development of that fuel as a competitive alternative.

Protecting American consumers from anticompetitive practices in the energy sector has long been one of our top priorities, and I can assure you that we will evaluate POP Diesel's concerns under pertinent antitrust standards.

Thank you again for raising this topic with me. The Commission continues to make every effort to identify, pursue, and prevent practices in energy and other markets that violate any statute or rule that the agency enforces. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 8, 2014

The Honorable Tom Udall
United States Senate
Washington, D.C. 20510

Dear Senator Udall:

Thank you for the November 12, 2014 letter from you and Senator Heinrich requesting that the Commission give due consideration to concerns that New Mexico-based Plant Oil Powered Diesel Fuel Systems, Inc. ("POP Diesel") recently raised with the FTC about certain standard-setting decisions by ASTM International that it believes may be impeding competition.

You report that POP Diesel produces equipment that enables any diesel engine to run on 100 percent vegetable oil fuel, and that the company is aiming to establish a nationwide network of filling stations devoted to this fuel following the Environmental Protection Agency's approval last year of the use of such fuel with POP Diesel's technology. You also mention that state and federal authorities often incorporate ASTM's standards into legal requirements, and that the exclusion of pure plant oil from ASTM fuel standards could thus harm the development of that fuel as a competitive alternative.

Protecting American consumers from anticompetitive practices in the energy sector has long been one of our top priorities, and I can assure you that we will evaluate POP Diesel's concerns under pertinent antitrust standards.

Thank you again for raising this topic with me. The Commission continues to make every effort to identify, pursue, and prevent practices in energy and other markets that violate any statute or rule that the agency enforces. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 8, 2014

The Honorable John Lewis
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Lewis:

Thank you for your November 13, 2014 letter to the Department of Labor and the Federal Trade Commission regarding media reports of an emerging food service industry practice requiring non-compete agreements from rank-and-file workers. In particular, you express concern about reports that such provisions sometimes restrict rank-and-file employees from working for any competing food service company within a given geographical radius from the employer for up to two years after employment has ended, and that the provisions sometimes designate a broad group of local businesses as competitors. You ask that the Commission look into these reports and consider whether any such non-compete agreements may harm competition in labor markets.

With respect to the competition issues you have raised, I can assure you that we will evaluate the information you have provided and the concerns you have expressed. The Commission continues to make every effort to identify, pursue, and prevent practices in the marketplace that violate any statute or rule that the agency enforces. I should also note that non-compete agreements may be unenforceable under the laws of some states, and you may therefore also want to consider sharing your concerns with State Attorneys General. With respect to the permissibility of the agreements you describe under federal labor law, we will defer to the expertise of the Department of Labor.

Thank you again for bringing your observations to my attention. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. I appreciate your interest and vigilance in maintaining competition in the marketplace. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 19, 2014

The Honorable Charles E. Schumer
United States Senate
Washington, DC 20510

Dear Senator Schumer:

Thank you for your letter regarding vulnerabilities associated with certain Internet Protocol (“IP”) cameras. In particular, you identified as a problematic practice device manufacturers using default passwords to secure IP cameras because this practice may expose consumers to unanticipated privacy intrusions. I appreciate your strong support for consumer privacy and data security, and I share your concerns about consumers’ exposure to harm from intruders exploiting vulnerable, Internet-connected devices.

Enabling ordinary devices to communicate with each other and with consumers over the Internet has led to important innovation in consumer products and services. It is critical, however, that companies prioritize privacy and security as they develop devices that connect to the Internet. The Commission has undertaken a number of initiatives related to Internet-connected devices, including IP cameras. Late last year, the Commission held a public workshop that explored the privacy and security issues created by the growing connectivity of devices.¹ We sought public comment both before and after the workshop, and we plan to issue a staff report of the proceedings soon.

The FTC also has issued guidance addressing some of the security risks created by Internet-connected devices. For example, our consumer guidance provides tips to help consumers prevent and respond to security issues affecting IP cameras.² In conjunction with our forthcoming report, FTC staff is preparing additional guidance for industry, and we expect that it will address default passwords in Internet-connected devices.

Finally, the Commission is committed to using its enforcement authority against companies that fail to take reasonable steps to develop and maintain secure IP cameras and other

¹ INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, *available at* <http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world>.

² “Using IP Cameras Safely,” FEDERAL TRADE COMMISSION (Sept. 2013), <http://www.consumer.ftc.gov/articles/0382-using-ip-cameras-safely>.

Internet-connected devices. For example, earlier this year, the Commission finalized its settlement with TRENDnet, Inc., a retailer of IP cameras to home users and to small- and medium-sized businesses.³ The Commission charged TRENDnet with engaging in unfair and deceptive practices because its cameras were vulnerable to online viewing, and in some instances listening, by anyone with the cameras' IP addresses. Similar to the recent events detailed in your letter, the Commission's complaint alleged that an attacker exploited and publicized this flaw, and other attackers posted links to the live feeds of nearly 700 cameras. The Commission's order requires, among other things, that TRENDnet implement a comprehensive security program to protect data and address security risks that could lead to unauthorized access to any of the company's Internet-connected products, including IP cameras.

The Commission is continuing its work to protect consumers using Internet-connected devices, including IP cameras, through its enforcement activities, outreach to consumers and industry, and monitoring of the marketplace.

If you or your staff have additional questions on these matters or wish to share additional information with us, please do not hesitate to contact me or have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at 202-326-2946.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Edith Ramirez', with a stylized flourish at the end.

Edith Ramirez
Chairwoman

³ *In re TRENDnet, Inc.*, FTC File No. 1223090 (F.T.C. Feb. 7, 2014) (final consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 22, 2014

The Honorable Karen Bass
U.S. House of Representatives
Washington, D.C. 20515

Dear Representative Bass:

Thank you for your December 15, 2014 letter on behalf of your constituents regarding the proposed merger of the Albertsons and Safeway supermarket chains. I appreciate receiving the information and views presented in your correspondence concerning the importance of preserving supermarket competition, particularly in an urban area where your constituents may have limited options.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the disclosure of the details of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction.¹ I can assure you that, as in all our merger reviews, the Commission is committed to conducting a thorough investigation of competitive effects in all relevant markets likely to be affected by the transaction. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you again for bringing your constituents' concerns to our attention in this important matter. As always, we appreciate your interest and vigilance in maintaining competition and protecting consumers in the marketplace. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman

¹ *Federal Trade Commission Notice of Policy of Disclosing Investigations of Announced Mergers: Notice of Revised Policy*, 62 Fed. Reg. 18630 (Apr. 16, 1997); see also *Federal Trade Commission Policy Concerning Disclosures of Nonmerger Competition and Consumer Protection Investigations: Notice of Revised Policy*, 63 Fed. Reg. 63477 (Nov. 13, 1998).



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 22, 2014

The Honorable Jeffrey A. Merkley
United States Senate
Washington, D.C. 20510

Dear Senator Merkley:

Thank you for the December 8, 2014 letter from you and Senator Wyden regarding the proposed merger of AB Acquisition LLC and Safeway, Inc. I appreciate receiving the information and views presented in your correspondence concerning the importance of preserving supermarket competition in small communities that may be affected by the proposed merger, including Baker County, Oregon.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the disclosure of the details of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction.¹ I can assure you that, as in all our merger reviews, the Commission is committed to conducting a thorough investigation of competitive effects in all relevant markets likely to be affected by the transaction. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you again for bringing your observations to our attention in this important matter. As always, we appreciate your interest and vigilance in maintaining competition and protecting consumers in the marketplace. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman

¹ *Federal Trade Commission Notice of Policy of Disclosing Investigations of Announced Mergers: Notice of Revised Policy*, 62 Fed. Reg. 18630 (Apr. 16, 1997); see also *Federal Trade Commission Policy Concerning Disclosures of Nonmerger Competition and Consumer Protection Investigations: Notice of Revised Policy*, 63 Fed. Reg. 63477 (Nov. 13, 1998).



OFFICE OF THE
CHAIRWOMAN

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON D.C. 20580

December 22, 2014

The Honorable Ron Wyden
United States Senate
Washington, D.C. 20510

Dear Senator Wyden:

Thank you for the December 8, 2014 letter from you and Senator Merkley regarding the proposed merger of AB Acquisition LLC and Safeway, Inc. I appreciate receiving the information and views presented in your correspondence concerning the importance of preserving supermarket competition in small communities that may be affected by the proposed merger, including Baker County, Oregon.

As you know, a number of statutory prohibitions and the Rules of the Commission prevent the disclosure of the details of any nonpublic investigation, but I am able to confirm that the Commission is conducting an investigation of the proposed transaction.¹ I can assure you that, as in all our merger reviews, the Commission is committed to conducting a thorough investigation of competitive effects in all relevant markets likely to be affected by the transaction. Members of the Commission staff will promptly publicize any public action that the Commission or its staff may take with respect to the Commission investigation.

Thank you again for bringing your observations to our attention in this important matter. As always, we appreciate your interest and vigilance in maintaining competition and protecting consumers in the marketplace. If you or your staff have any questions, please feel free to have your staff call Jeanne Bumpus, the Director of our Office of Congressional Relations, at (202) 326-2195. Please also let me know if we can be of further service in this or any other matter.

Sincerely,

Edith Ramirez
Chairwoman

¹ *Federal Trade Commission Notice of Policy of Disclosing Investigations of Announced Mergers: Notice of Revised Policy*, 62 Fed. Reg. 18630 (Apr. 16, 1997); see also *Federal Trade Commission Policy Concerning Disclosures of Nonmerger Competition and Consumer Protection Investigations: Notice of Revised Policy*, 63 Fed. Reg. 63477 (Nov. 13, 1998).