The author’s views are his or her own, and do not necessarily represent the views of the Commission or any Commissioner.

Informing (public) policy

Lorrie Faith Cranor

Chief Technologist

US Federal Trade Commission

Carnegie Mellon University

privacy ENGINEERING

CyLab Usable Privacy & Security Laboratory

HTTP://CUPS.CS.CMU.EDU

©2006 Ral

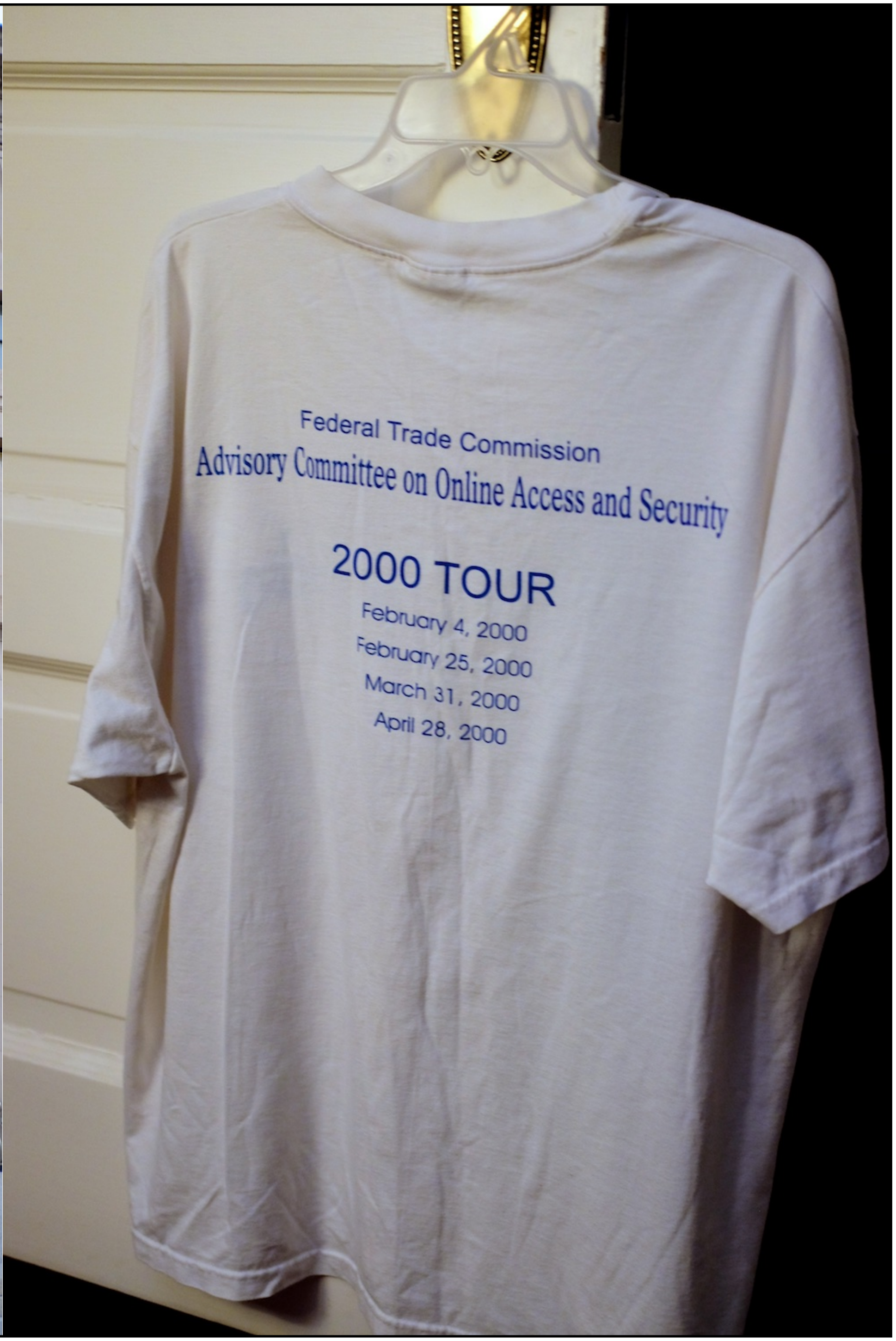
Today’s agenda

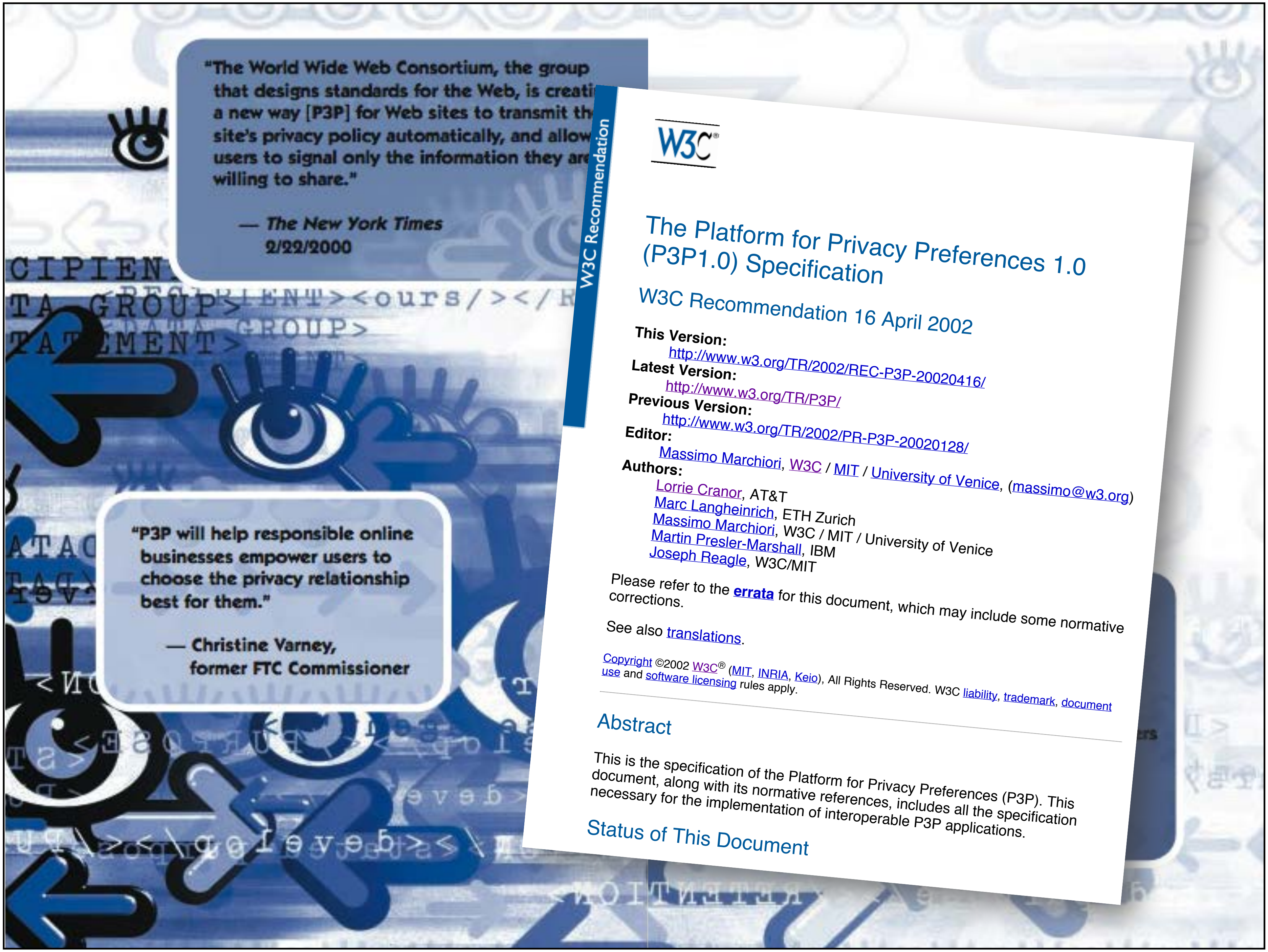
- How I got involved in public policy work
- What have I been doing at the FTC?
  - Password expiry
  - Police open data
  - Mobile account hijacking
  - Disclosures
- Opportunities for researchers to inform policy

Washington University in St. Louis

AT&T Labs-Research

FEDERAL TRADE
COMMISSION


Federal Trade Commission
Advisory Committee on Online Access and Security
2000 TOUR
February 4, 2000
February 25, 2000
March 31, 2000
April 28, 2000



"The World Wide Web Consortium, the group that designs standards for the Web, is creati a new way [P3P] for Web sites to transmit th site's privacy policy automatically, and allow users to signal only the information they are willing to share."

— *The New York Times* 2/22/2000

"P3P will help responsible online businesses empower users to choose the privacy relationship best for them."

— Christine Varney, former FTC Commissioner

W3C Recommendation

The Platform for Privacy Preferences 1.0 (P3P1.0) Specification

W3C Recommendation 16 April 2002

This Version:
http://www.w3.org/TR/2002/REC-P3P-20020416/
Latest Version:
http://www.w3.org/TR/P3P/
Previous Version:
http://www.w3.org/TR/2002/PR-P3P-20020128/
Editor:
Massimo Marchiori, W3C / MIT / University of Venice, (massimo@w3.org)
Authors:
Lorrie Cranor, AT&T
Marc Langheinrich, ETH Zurich
Massimo Marchiori, W3C / MIT / University of Venice
Martin Presler-Marshall, IBM
Joseph Reagle, W3C/MIT

Please refer to the **errata** for this document, which may include some normative corrections.

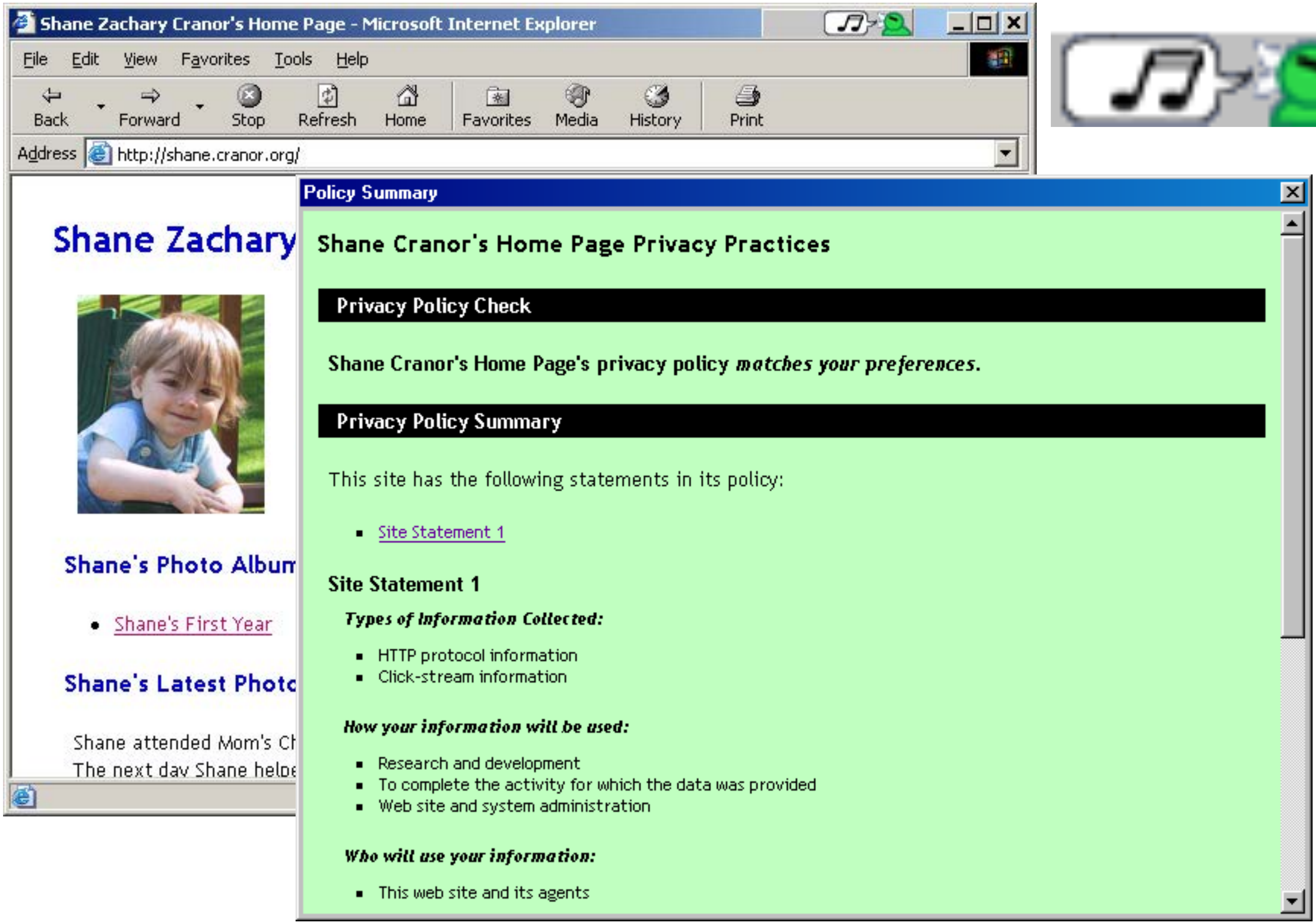
See also translations.

Copyright ©2002 W3C® (MIT, INRIA, Keio), All Rights Reserved. W3C liability, trademark, document use and software licensing rules apply.

Abstract

This is the specification of the Platform for Privacy Preferences (P3P). This document, along with its normative references, includes all the specification necessary for the implementation of interoperable P3P applications.

Status of This Document


Shane Zachary Cranor's Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Favorites Media History Print
Address http://shane.cranor.org/
Policy Summary

Shane Zachary

Shane's Photo Albur

- Shane's First Year

Shane's Latest Photo

Shane attended Mom's Cl
The next dav Shane helpe

Shane Cranor's Home Page Privacy Practices

Privacy Policy Check

Shane Cranor's Home Page's privacy policy *matches your preferences.*

Privacy Policy Summary

This site has the following statements in its policy:

- Site Statement 1

Site Statement 1

Types of Information Collected:

- HTTP protocol information
- Click-stream information

How your information will be used:

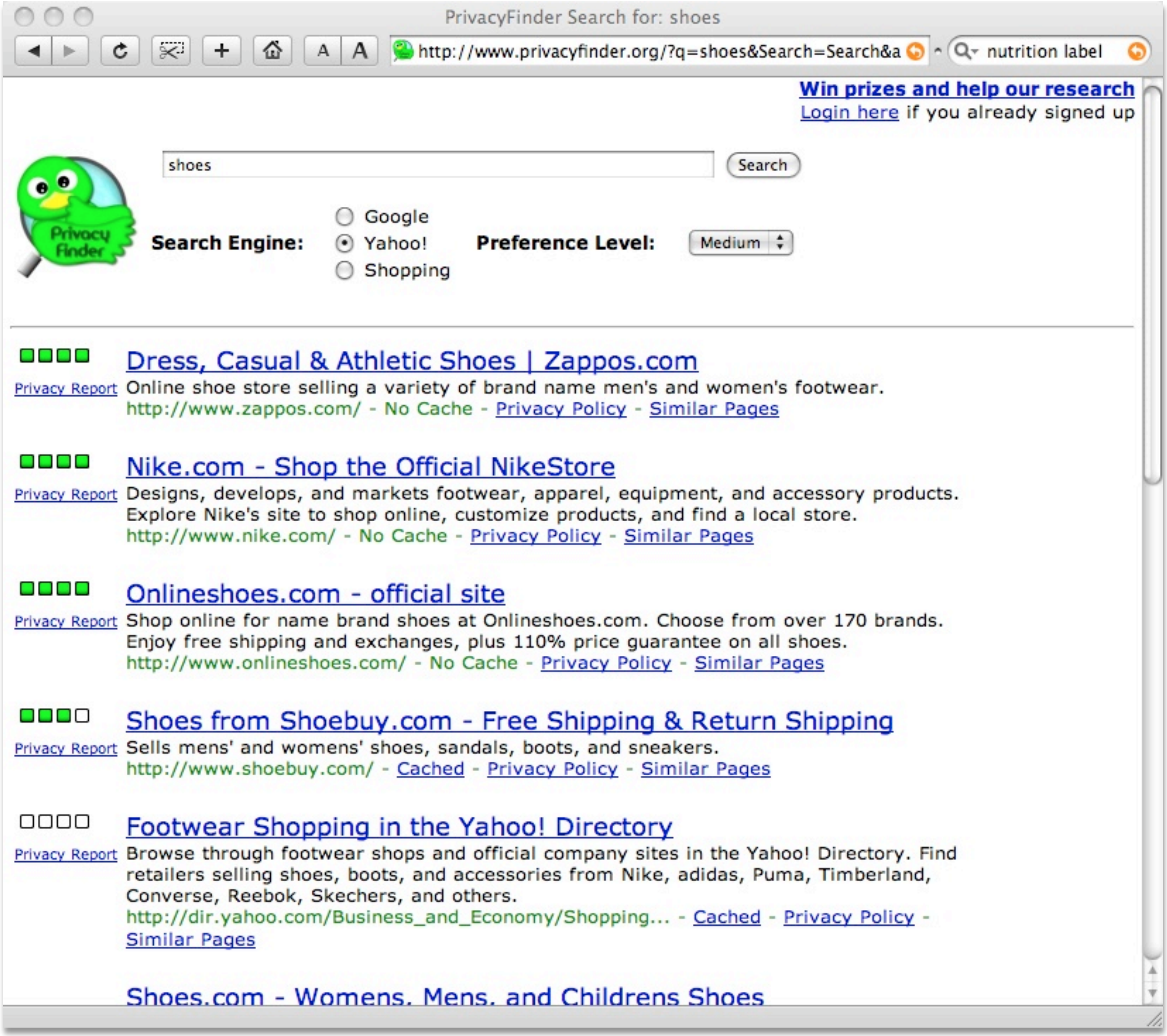
- Research and development
- To complete the activity for which the data was provided
- Web site and system administration

Who will use your information:

- This web site and its agents

Carnegie Mellon University

CUPS Lab 2007


PrivacyFinder Search for: shoes
http://www.privacyfinder.org/?q=shoes&Search=Search&a
nutrition label
Privacy Finder
Search

[Win prizes and help our research](#)
[Login here](#) if you already signed up

shoes

Search Engine: ○ Google ● Yahoo! ○ Shopping

Preference Level: Medium

🟩🟩🟩🟩 [Dress, Casual & Athletic Shoes | Zappos.com](#)
[Privacy Report](#) Online shoe store selling a variety of brand name men's and women's footwear.
http://www.zappos.com/ - No Cache - [Privacy Policy](#) - [Similar Pages](#)

🟩🟩🟩🟩 [Nike.com - Shop the Official NikeStore](#)
[Privacy Report](#) Designs, develops, and markets footwear, apparel, equipment, and accessory products. Explore Nike's site to shop online, customize products, and find a local store.
http://www.nike.com/ - No Cache - [Privacy Policy](#) - [Similar Pages](#)

🟩🟩🟩🟩 [Onlineshoes.com - official site](#)
[Privacy Report](#) Shop online for name brand shoes at Onlineshoes.com. Choose from over 170 brands. Enjoy free shipping and exchanges, plus 110% price guarantee on all shoes.
http://www.onlineshoes.com/ - No Cache - [Privacy Policy](#) - [Similar Pages](#)

🟩🟩🟩□ [Shoes from Shoebuy.com - Free Shipping & Return Shipping](#)
[Privacy Report](#) Sells mens' and womens' shoes, sandals, boots, and sneakers.
http://www.shoebuy.com/ - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

□□□□ [Footwear Shopping in the Yahoo! Directory](#)
[Privacy Report](#) Browse through footwear shops and official company sites in the Yahoo! Directory. Find retailers selling shoes, boots, and accessories from Nike, adidas, Puma, Timberland, Converse, Reebok, Skechers, and others.
http://dir.yahoo.com/Business_and_Economy/Shopping... - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

[Shoes.com - Womens, Mens, and Childrens Shoes](#)

Time to read policies of websites you visit: 244 hours/year

We have updated our Privacy Policy as of 10 June 2015.

SoundCloud Privacy Policy

Welcome to SoundCloud®, a service provided by SoundCloud Limited ("SoundCloud" "we" "our", "us").

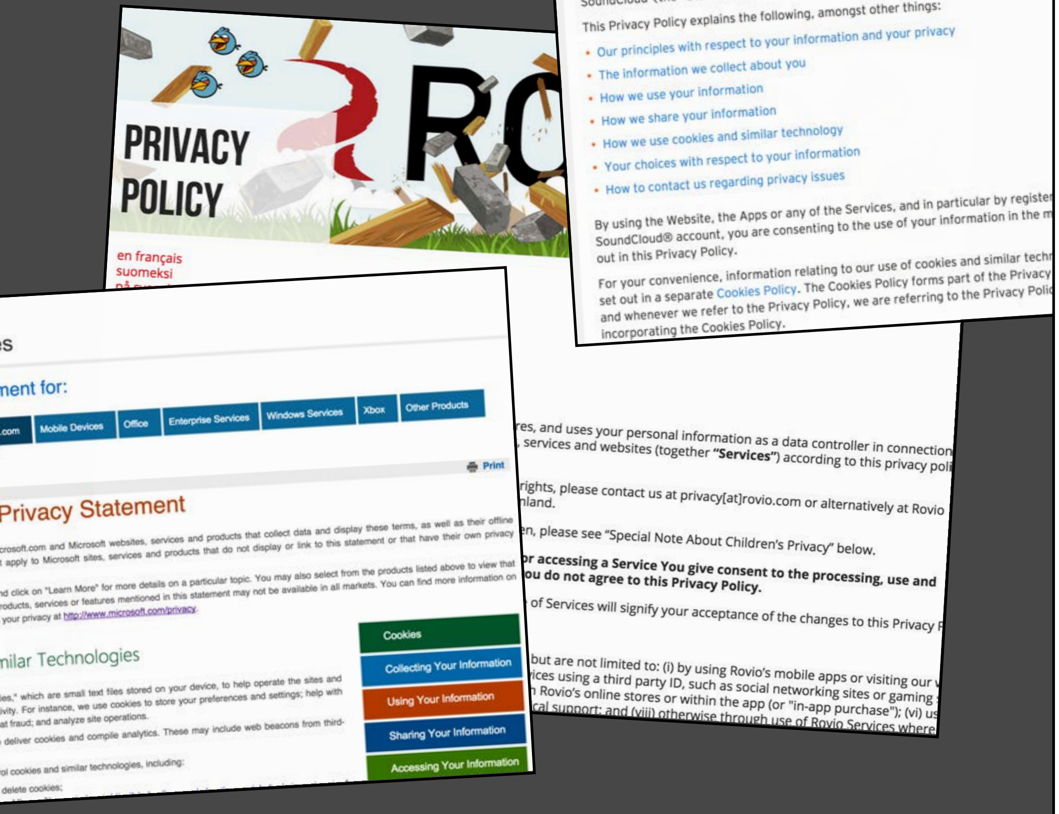
Your privacy is important to us. This Privacy Policy explains how we collect, store, us disclose your information when you use soundcloud.com and m.soundcloud.com (together, the "Website"), our mobile and desktop apps (the "Apps") and all relate sites, players, widgets, tools, apps, data, software, APIs and other services provided SoundCloud (the "Services").

This Privacy Policy explains the following, amongst other things:

- Our principles with respect to your information and your privacy
- The information we collect about you
- How we use your information
- How we share your information
- How we use cookies and similar technology
- Your choices with respect to your information
- How to contact us regarding privacy issues

By using the Website, the Apps or any of the Services, and in particular by register SoundCloud® account, you are consenting to the use of your information in the m out in this Privacy Policy.

For your convenience, information relating to our use of cookies and similar techn set out in a separate Cookies Policy. The Cookies Policy forms part of the Privacy and whenever we refer to the Privacy Policy, we are referring to the Privacy Polic incorporating the Cookies Policy.



Privacy Policy

January 1

Published: January 1, 2015

The WP Company LLC ("The Washington Post") recognizes the importa personal information, and we have prepar about our

res, and uses your personal information as a data controller in connection , services and websites (together "Services") according to this privacy poli

rights, please contact us at privacy[at]rovio.com or alternatively at Rovio nland.

en, please see "Special Note About Children's Privacy" below.

or accessing a Service You give consent to the processing, use and ou do not agree to this Privacy Policy.

of Services will signify your acceptance of the changes to this Privacy P

but are not limited to: (i) by using Rovio's mobile apps or visiting our v vices using a third party ID, such as social networking sites or gaming n Rovio's online stores or within the app (or "in-app purchase"); (vi) us cal support; and (viii) otherwise through use of Rovio Services where

Microsoft

Privacy & Cookies

View Privacy Statement for:

Last Updated: October 2014

Microsoft.com Privacy Statement

This privacy statement applies to Microsoft.com and Microsoft websites, services and products that collect data and display these terms, as well as their offline product support services. It does not apply to Microsoft sites, services and products that do not display or link to this statement or that have their own privacy statements.

Please read the summaries below and click on "Learn More" for more details on a particular topic. You may also select from the products listed above to view that product's privacy statement. Some products, services or features mentioned in this statement may not be available in all markets. You can find more information on Microsoft's commitment to protecting your privacy at http://www.microsoft.com/privacy.

Cookies & Similar Technologies

Most Microsoft websites use "cookies," which are small text files stored on your device, to help operate the sites and collect information about online activity. For instance, we use cookies to store your preferences and settings; help with sign-in; provide targeted ads; combat fraud; and analyze site operations.

We also use web beacons to help deliver cookies and compile analytics. These may include web beacons from third-party service providers.

You have a variety of tools to control cookies and similar technologies, including:

- Browser controls to block and delete cookies;

Cookies
Collecting Your Information
Using Your Information
Sharing Your Information
Accessing Your Information

Search Facebook
Florian
Ho
What kinds of information do we collect?
How do we use this information?
How is this information shared?
How can I manage or delete information about me?
How do we respond to legal requests or prevent harm?
How our global services operate
How will we notify you of changes to this policy?

Data Policy

We give you the power to share as part of our mission t world more open and connected. This policy describes information we collect and how it is used and shared. Yo additional tools and information at Privacy Basics.

As you review our policy, keep in mind that it applies to all brands, products and services that do not have a separate privacy policy or that link to this policy, which we call the "Facebook Services" or "Services."

A. McDonald & L. Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, 2008.

P. Kelley, J. Bresee, L. Cranor, and R. Reeder. A "Nutrition Label" for Privacy. SOUPS 2009.

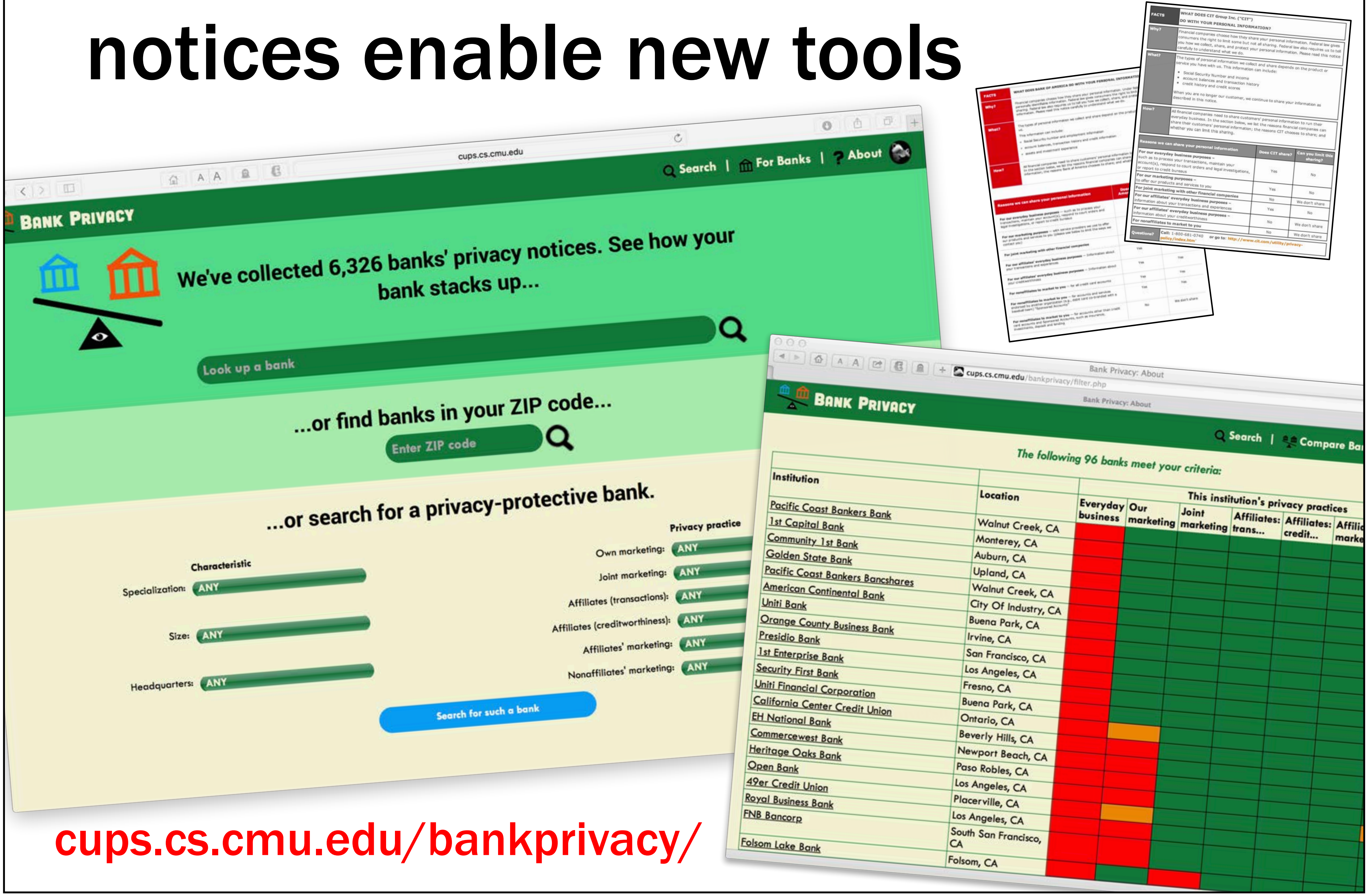
P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI 2010.

Privacy papers for policy makers

CHI 2012
Why Johnny Can't Opt Out:
A Usability Evaluation of
Tools to Limit Online
Behavioral Advertising

SOUPS 2012
Smart, Useful, Scary,
Creepy: Perceptions of
Online Behavioral
Advertising

Standardized financial privacy notices enable new tools



Bank Privacy

We've collected 6,326 banks' privacy notices. See how your bank stacks up...

...or find banks in your ZIP code...

...or search for a privacy-protective bank.

Characteristic	
Specialization:	ANY
Size:	ANY
Headquarters:	ANY

Privacy practice	
Own marketing:	ANY
Joint marketing:	ANY
Affiliates (transactions):	ANY
Affiliates (creditworthiness):	ANY
Affiliates' marketing:	ANY
Nonaffiliates' marketing:	ANY

WHAT DOES BANK OF AMERICA DO WITH YOUR PERSONAL INFORMATION

FACTS	WHAT DOES CIT Group Inc. ("CIT") DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depends on the product or service you have with us. This information can include: • Social Security Number and income • account balances and transaction history • credit history and credit scores When you are no longer our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons CIT chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does CIT share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

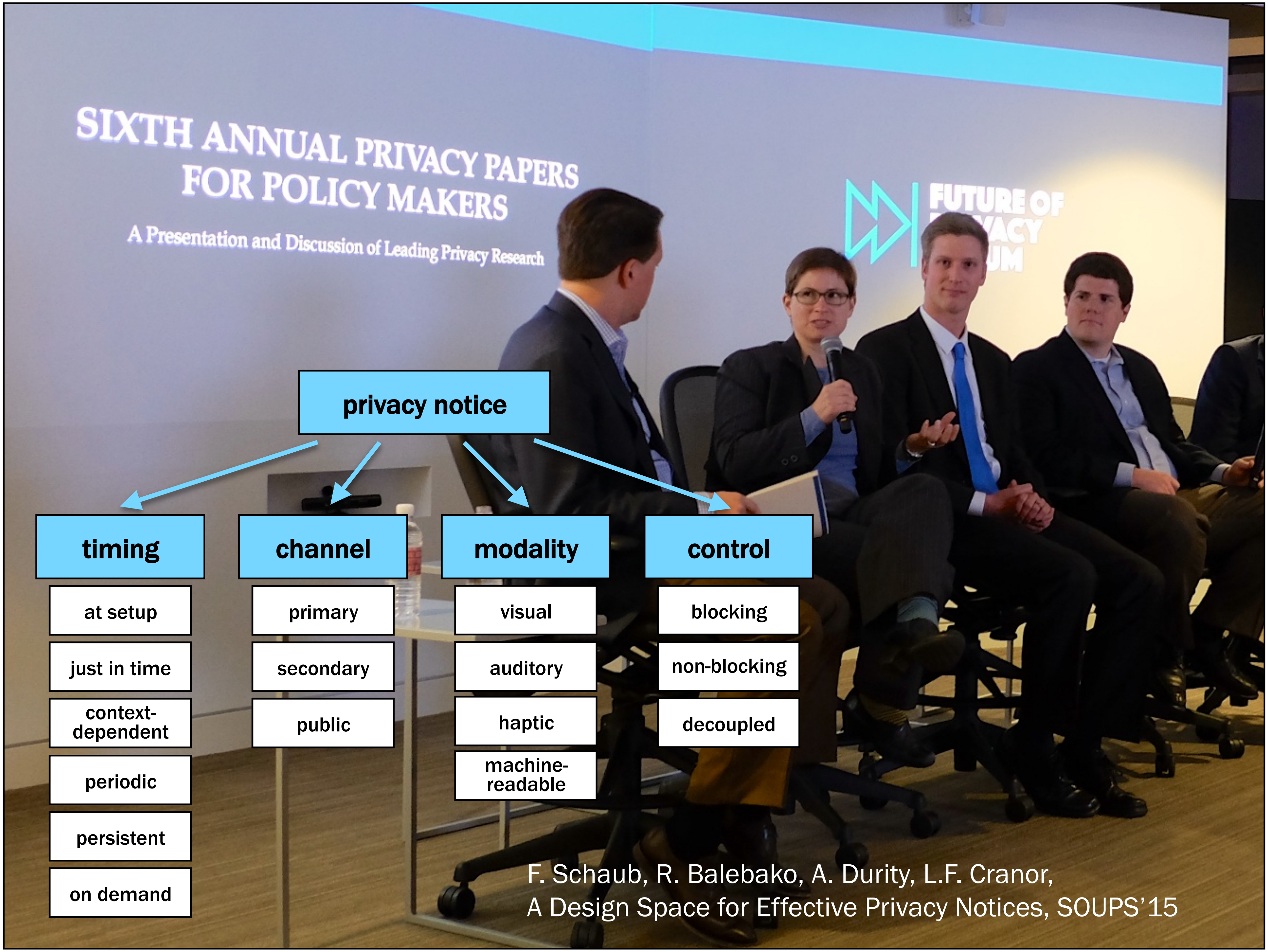
Questions? Call: 1-800-681-0740 or go to: http://www.cit.com/utility/privacy-policy/index.htm'

Bank Privacy

The following 96 banks meet your criteria:

Institution	Location	This institution's privacy practices					
		Everyday business	Our marketing	Joint marketing	Affiliates: trans...	Affiliates: credit...	Affili marke
Pacific Coast Bankers Bank	Walnut Creek, CA	🟥	🟩	🟩	🟩	🟩	🟩
1st Capital Bank	Monterey, CA	🟥	🟩	🟩	🟩	🟩	🟩
Community 1st Bank	Auburn, CA	🟥	🟩	🟩	🟩	🟩	🟩
Golden State Bank	Upland, CA	🟥	🟩	🟩	🟩	🟩	🟩
Pacific Coast Bankers Bancshares	Walnut Creek, CA	🟥	🟩	🟩	🟩	🟩	🟩
American Continental Bank	City Of Industry, CA	🟥	🟩	🟩	🟩	🟩	🟩
Uniti Bank	Buena Park, CA	🟥	🟩	🟩	🟩	🟩	🟩
Orange County Business Bank	Irvine, CA	🟥	🟩	🟩	🟩	🟩	🟩
Presidio Bank	San Francisco, CA	🟥	🟩	🟩	🟩	🟩	🟩
1st Enterprise Bank	Los Angeles, CA	🟥	🟩	🟩	🟩	🟩	🟩
Security First Bank	Fresno, CA	🟥	🟩	🟩	🟩	🟩	🟩
Uniti Financial Corporation	Buena Park, CA	🟥	🟩	🟩	🟩	🟩	🟩
California Center Credit Union	Ontario, CA	🟥	🟩	🟩	🟩	🟩	🟩
EH National Bank	Beverly Hills, CA	🟥	🟧	🟩	🟩	🟩	🟩
Commercewest Bank	Newport Beach, CA	🟥	🟥	🟩	🟩	🟩	🟩
Heritage Oaks Bank	Paso Robles, CA	🟥	🟥	🟩	🟩	🟩	🟩
Open Bank	Los Angeles, CA	🟥	🟥	🟩	🟩	🟩	🟩
49er Credit Union	Placerville, CA	🟥	🟥	🟩	🟩	🟩	🟩
Royal Business Bank	Los Angeles, CA	🟥	🟧	🟩	🟩	🟩	🟩
FNB Bancorp	South San Francisco, CA	🟥	🟥	🟩	🟩	🟩	🟧
Folsom Lake Bank	Folsom, CA	🟥	🟩	🟥	🟩	🟩	🟩

<span style="color:red">cups.cs.cmu.edu/bankprivacy/</span>


SIXTH ANNUAL PRIVACY PAPERS
FOR POLICY MAKERS
A Presentation and Discussion of Leading Privacy Research
FUTURE OF

privacy notice

timing	channel	modality	control
at setup	primary	visual	blocking
just in time	secondary	auditory	non-blocking
context-dependent	public	haptic	decoupled
periodic		machine-readable	
persistent			
on demand			

F. Schaub, R. Balebako, A. Durity, L.F. Cranor,
A Design Space for Effective Privacy Notices, SOUPS'15

FEDERAL
TRADE
COMMISSION
BUILDING
VISITORS ENTRANCE
6TH & PENN. AVE
♿ ENTRANCE
7TH & PENN AVE

Former Commissioner Julie Brill

Chairwoman Edith Ramirez

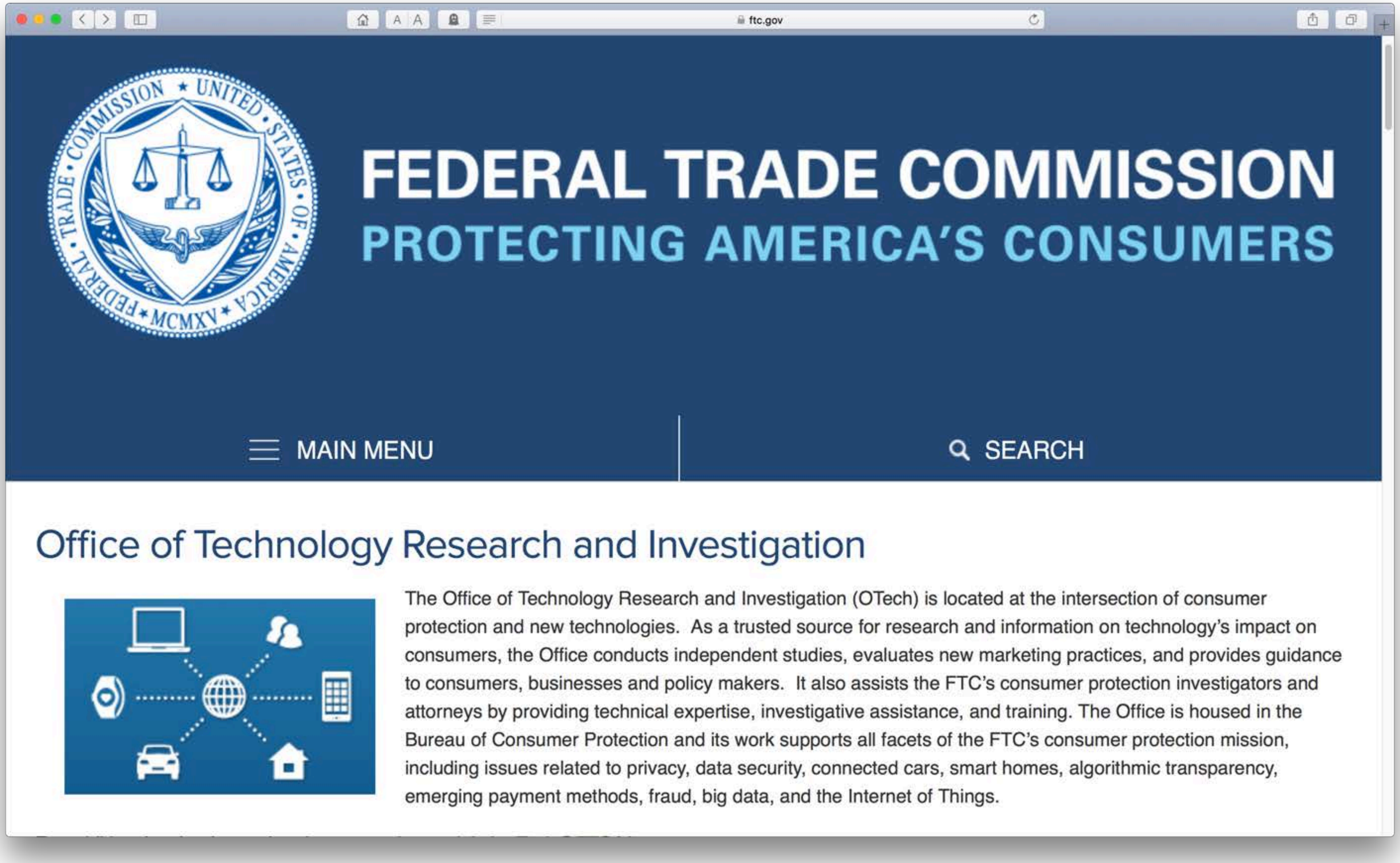
Commissioner Maureen Ohlhausen

Commissioner Terrell McSweeny

Jessica Rich
Bureau of Consumer Protection

Deborah Feinstein
Bureau of Competition

Ginger Jin
Bureau of Economics



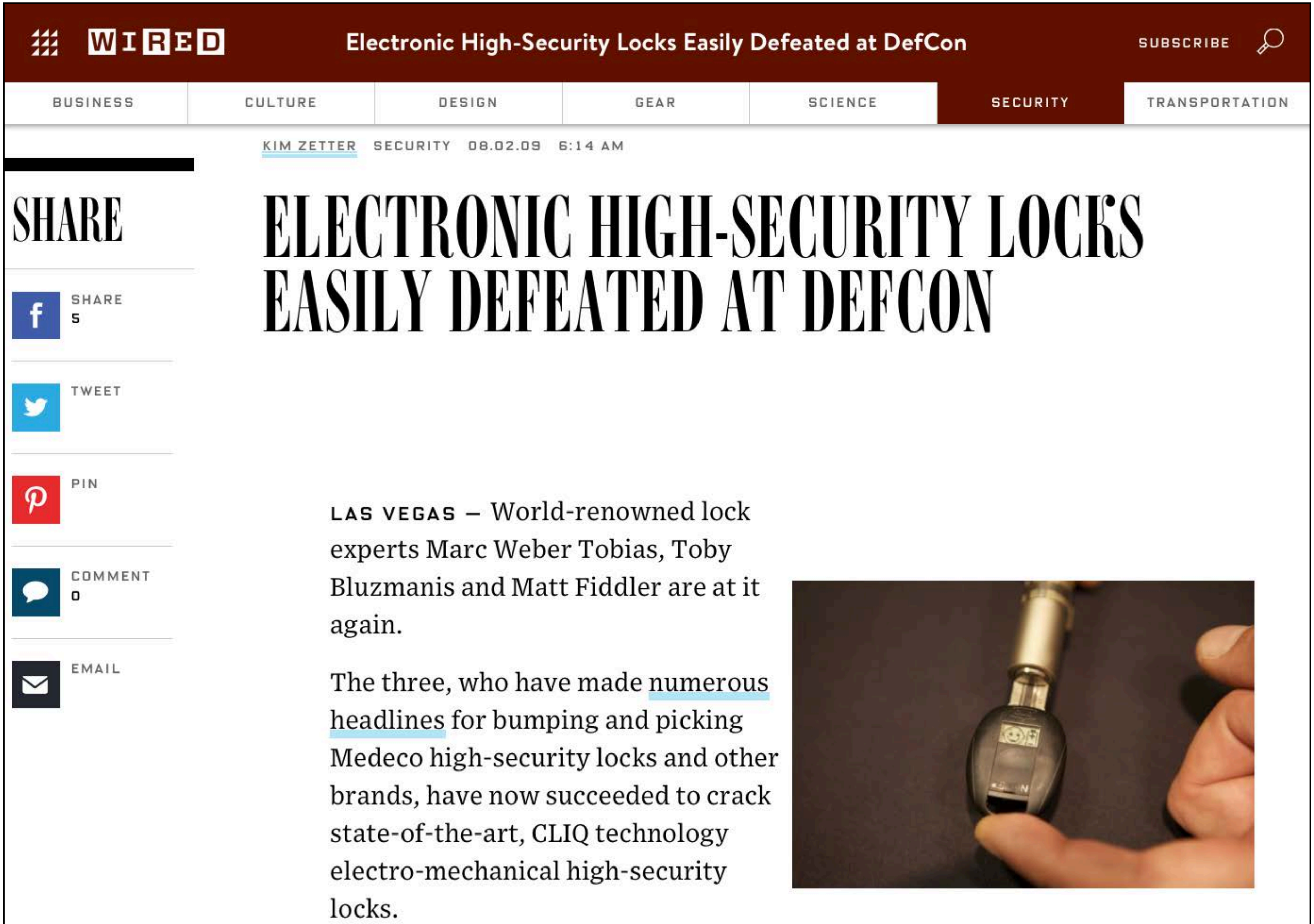
Office of Technology Research and Investigation

The Office of Technology Research and Investigation (OTech) is located at the intersection of consumer protection and new technologies. As a trusted source for research and information on technology's impact on consumers, the Office conducts independent studies, evaluates new marketing practices, and provides guidance to consumers, businesses and policy makers. It also assists the FTC's consumer protection investigators and attorneys by providing technical expertise, investigative assistance, and training. The Office is housed in the Bureau of Consumer Protection and its work supports all facets of the FTC's consumer protection mission, including issues related to privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, fraud, big data, and the Internet of Things.

357

CLIQ
medeco
CL150562

medeco



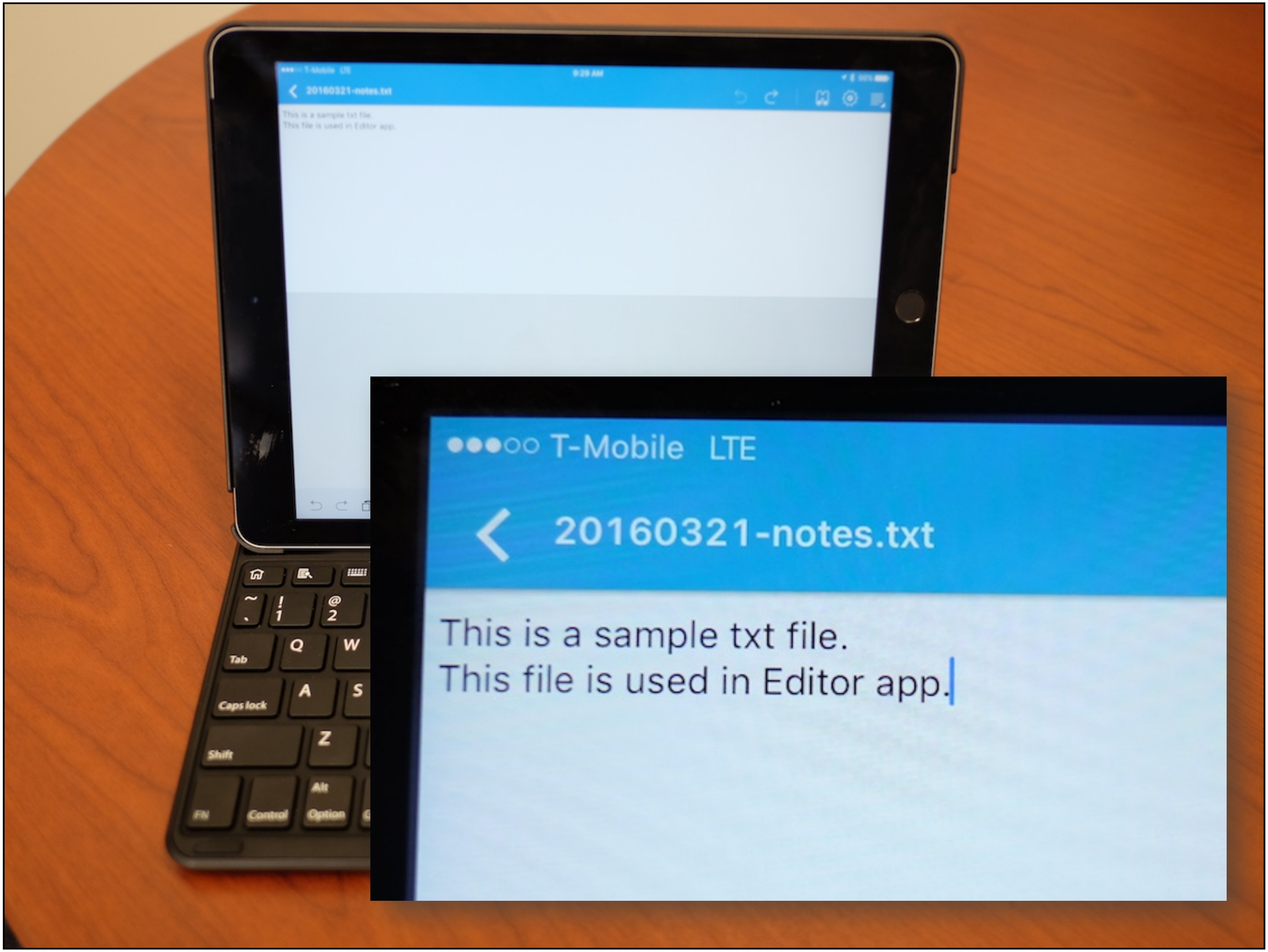
Electronic High-Security Locks Easily Defeated at DefCon

KIM ZETTER SECURITY 08.02.09 6:14 AM

ELECTRONIC HIGH-SECURITY LOCKS EASILY DEFEATED AT DEFCON

LAS VEGAS — World-renowned lock experts Marc Weber Tobias, Toby Bluzmanis and Matt Fiddler are at it again.

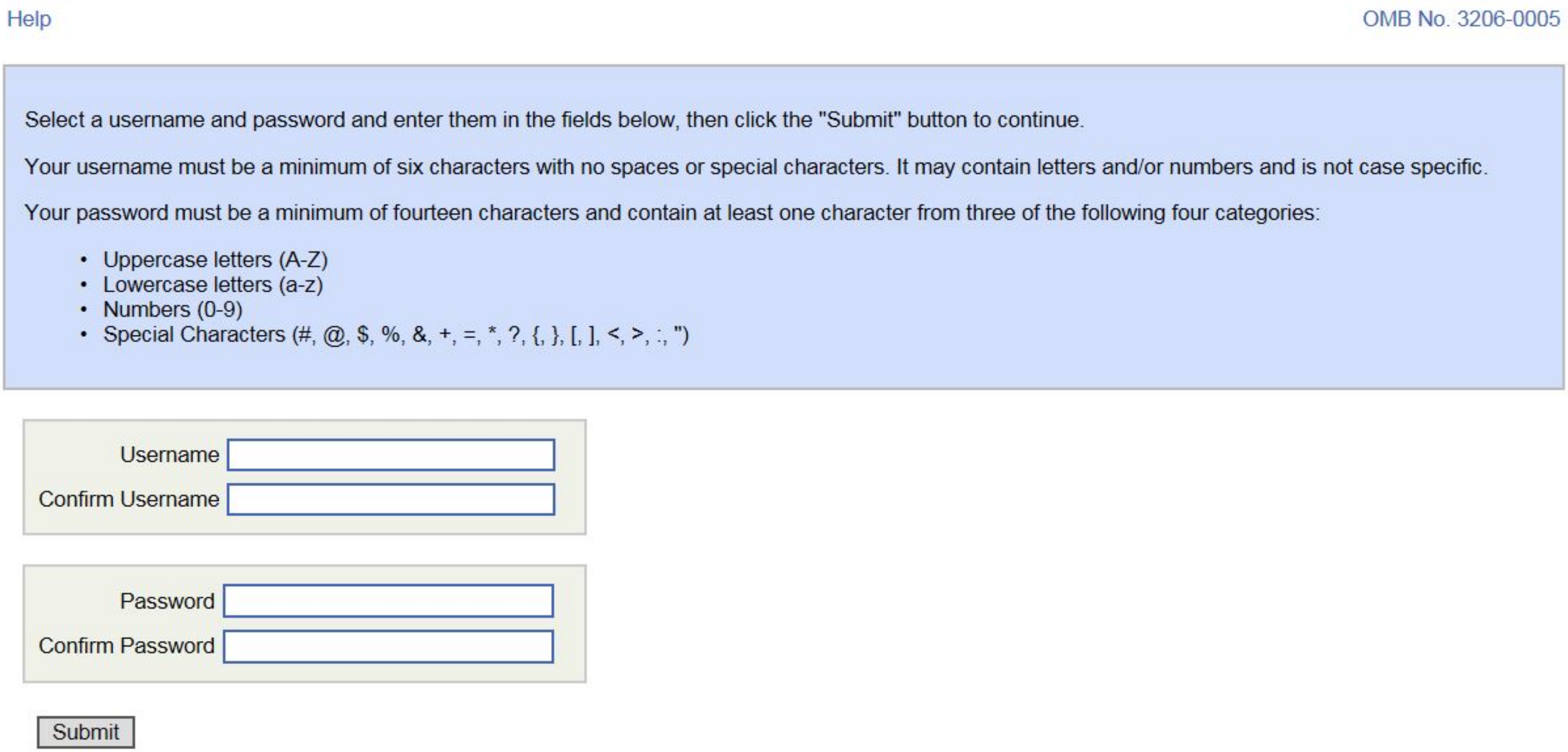
The three, who have made numerous headlines for bumping and picking Medeco high-security locks and other brands, have now succeeded to crack state-of-the-art, CLIQ technology electro-mechanical high-security locks.



This is a sample txt file.
This file is used in Editor app.

I created 6 new passwords during my first week at the FTC

14+ characters, 3 classes



Select a username and password and enter them in the fields below, then click the "Submit" button to continue.

Your username must be a minimum of six characters with no spaces or special characters. It may contain letters and/or numbers and is not case specific.

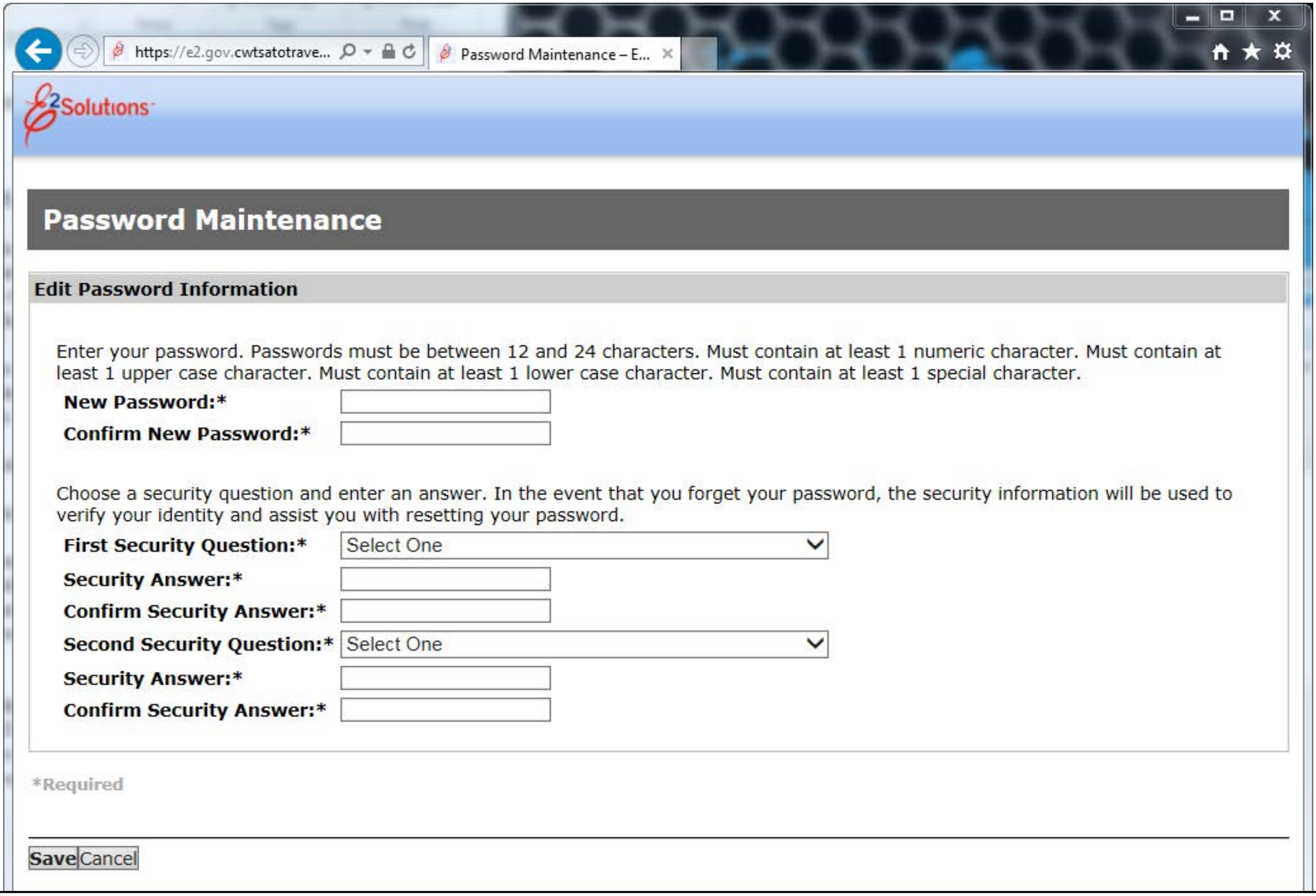
Your password must be a minimum of fourteen characters and contain at least one character from three of the following four categories:

- Uppercase letters (A-Z)
- Lowercase letters (a-z)
- Numbers (0-9)
- Special Characters (#, @, $, %, &, +, =, *, ?, {, }, [,], <, >, :, ")

Username	
Confirm Username	

Password	
Confirm Password	

12+ characters, 4 classes



Password Maintenance

Edit Password Information

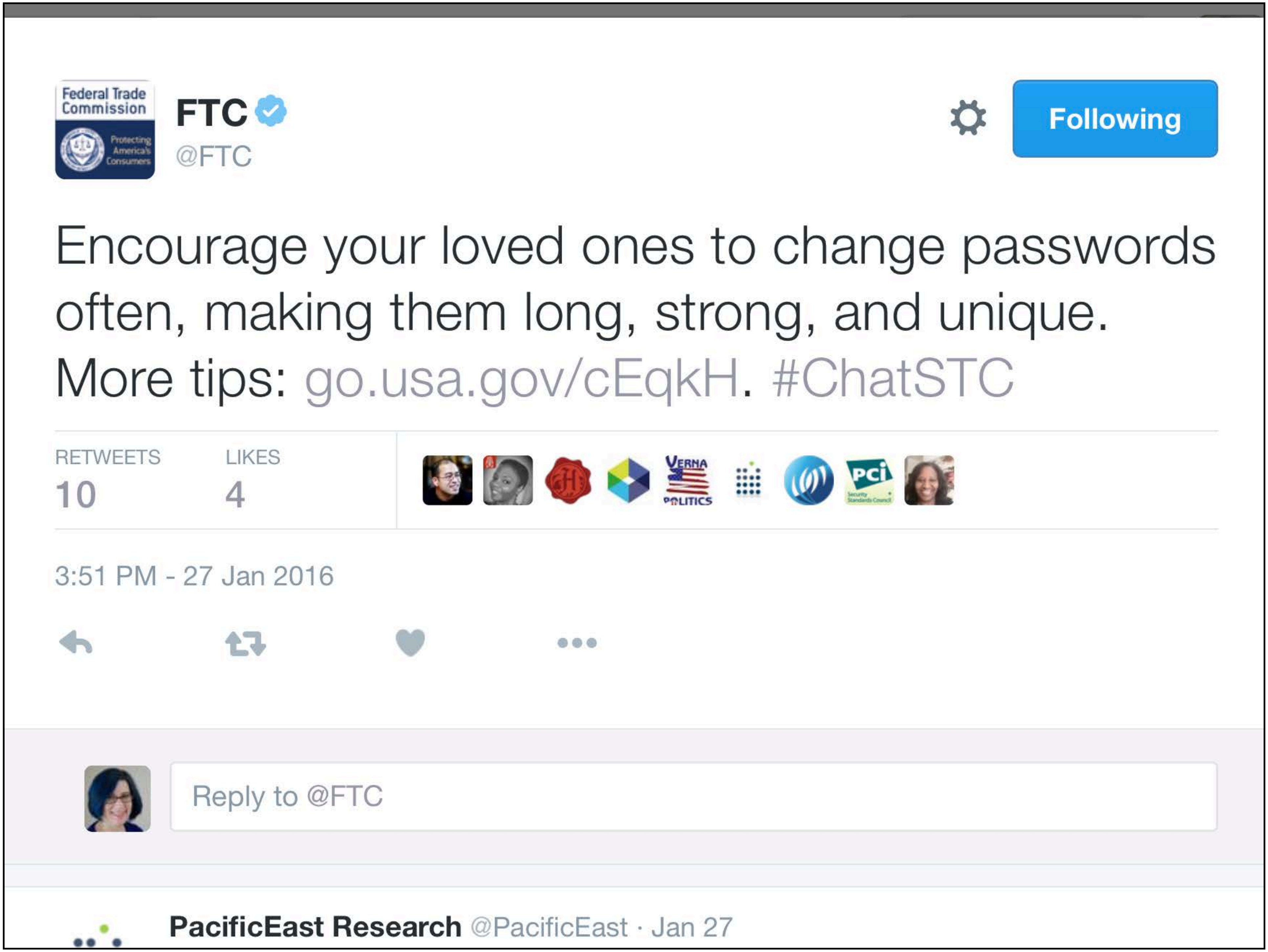
Enter your password. Passwords must be between 12 and 24 characters. Must contain at least 1 numeric character. Must contain at least 1 upper case character. Must contain at least 1 lower case character. Must contain at least 1 special character.

New Password:*	
Confirm New Password:*	

Choose a security question and enter an answer. In the event that you forget your password, the security information will be used to verify your identity and assist you with resetting your password.

First Security Question:*	Select One
Security Answer:*	
Confirm Security Answer:*	
Second Security Question:*	Select One
Security Answer:*	
Confirm Security Answer:*	

*Required



FTC @FTC

Encourage your loved ones to change passwords often, making them long, strong, and unique. More tips: go.usa.gov/cEqkH. #ChatSTC

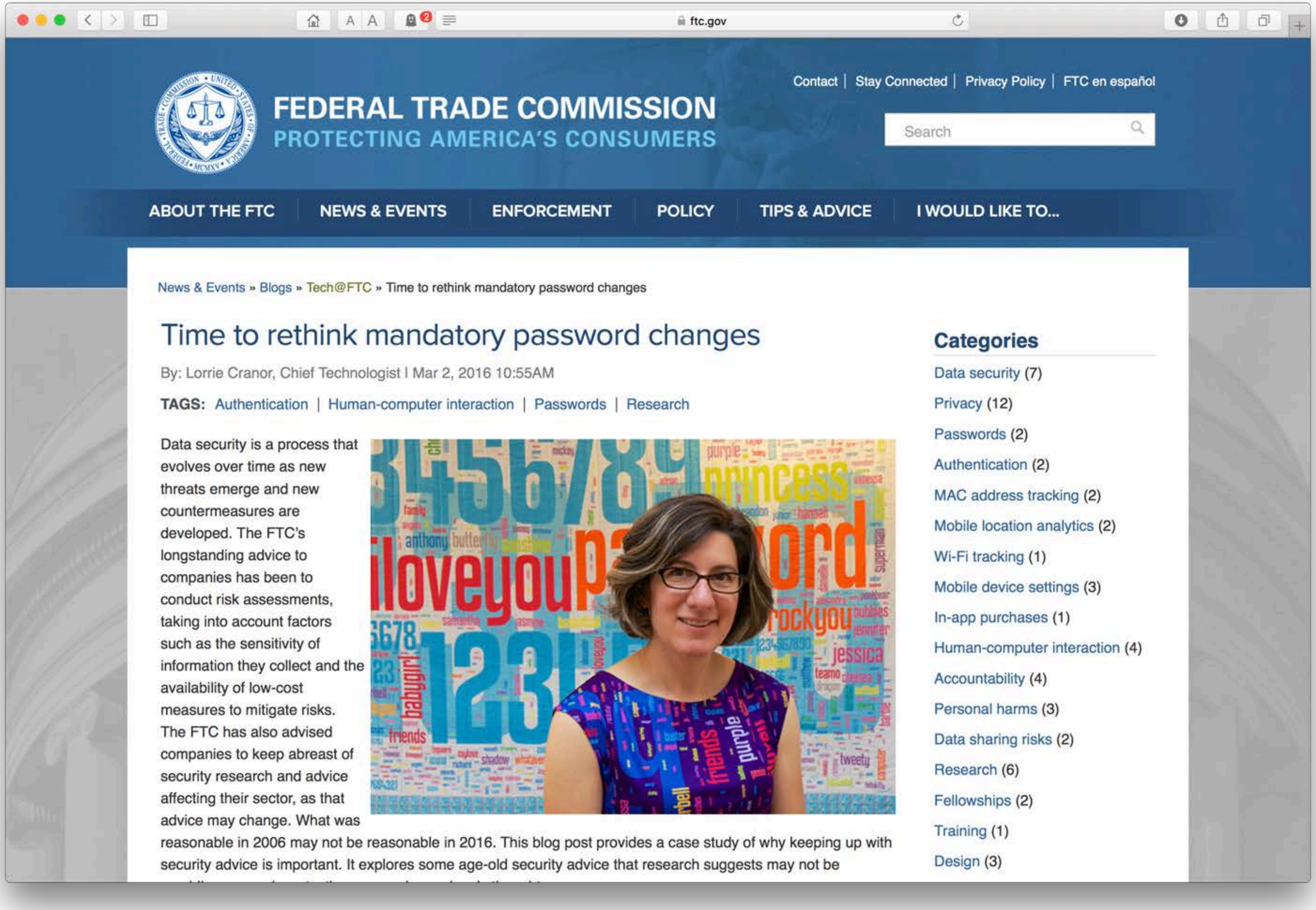
RETWEETS 10

LIKES 4

3:51 PM - 27 Jan 2016

Reply to @FTC

PacificEast Research @PacificEast · Jan 27


ftc.gov
Contact | Stay Connected | Privacy Policy | FTC en español
FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS
Search
ABOUT THE FTC
NEWS & EVENTS
ENFORCEMENT
POLICY
TIPS & ADVICE
I WOULD LIKE TO...
News & Events » Blogs » Tech@FTC » Time to rethink mandatory password changes

Time to rethink mandatory password changes

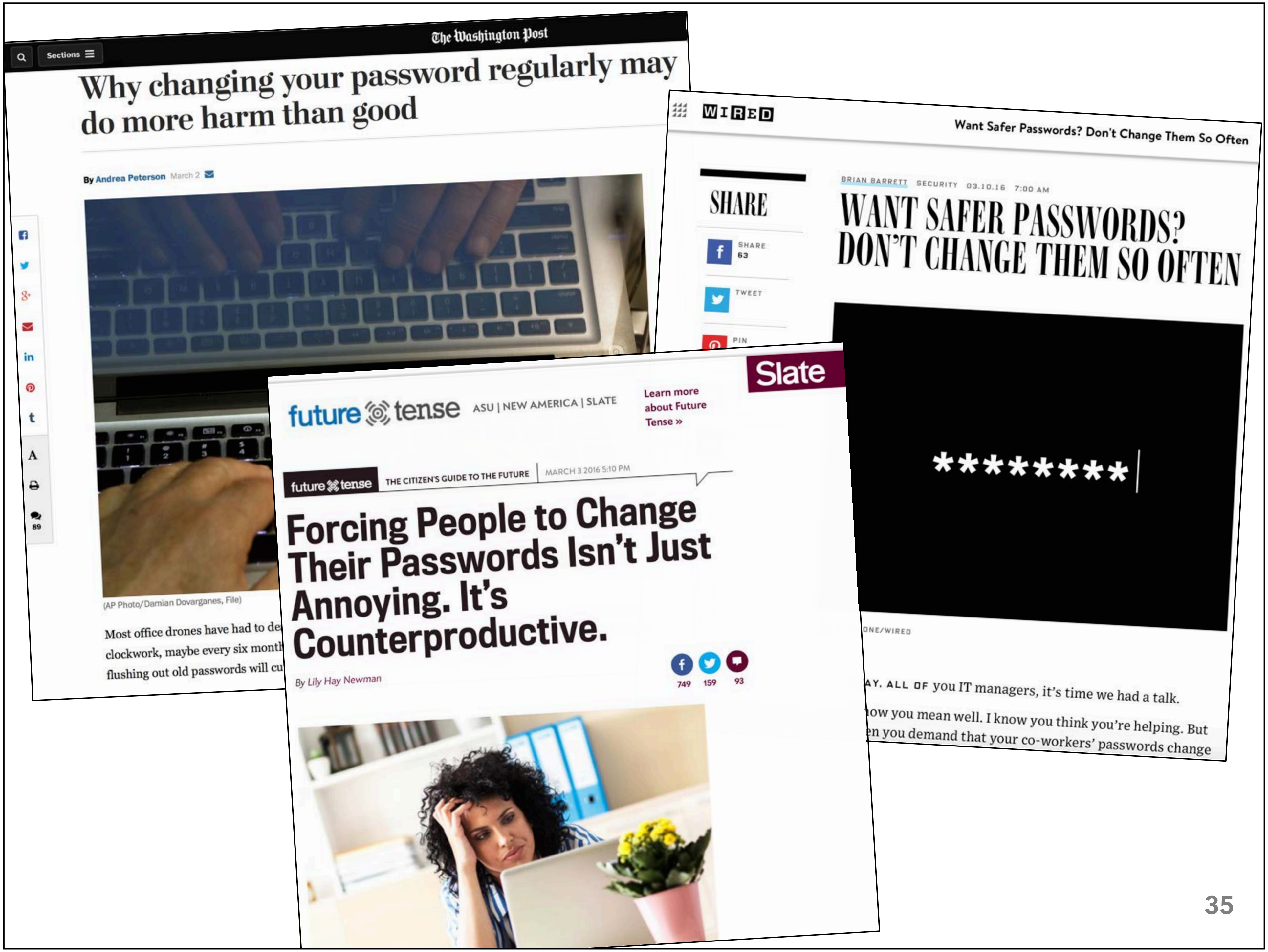
By: Lorrie Cranor, Chief Technologist | Mar 2, 2016 10:55AM

TAGS: Authentication | Human-computer interaction | Passwords | Research

Data security is a process that evolves over time as new threats emerge and new countermeasures are developed. The FTC's longstanding advice to companies has been to conduct risk assessments, taking into account factors such as the sensitivity of information they collect and the availability of low-cost measures to mitigate risks. The FTC has also advised companies to keep abreast of security research and advice affecting their sector, as that advice may change. What was reasonable in 2006 may not be reasonable in 2016. This blog post provides a case study of why keeping up with security advice is important. It explores some age-old security advice that research suggests may not be

Categories

- Data security (7)
- Privacy (12)
- Passwords (2)
- Authentication (2)
- MAC address tracking (2)
- Mobile location analytics (2)
- Wi-Fi tracking (1)
- Mobile device settings (3)
- In-app purchases (1)
- Human-computer interaction (4)
- Accountability (4)
- Personal harms (3)
- Data sharing risks (2)
- Research (6)
- Fellowships (2)
- Training (1)
- Design (3)



The Washington Post

Sections

Why changing your password regularly may do more harm than good

By Andrea Peterson March 2

89

(AP Photo/Damian Dovarganes, File)

Most office drones have had to de
clockwork, maybe every six month
flushing out old passwords will cu

WIRED

Want Safer Passwords? Don't Change Them So Often

SHARE

SHARE 63

TWEET

PIN

BRIAN BARRETT SECURITY 03.10.16 7:00 AM

WANT SAFER PASSWORDS? DON'T CHANGE THEM SO OFTEN

****

ONE/WIRED

AY. ALL OF you IT managers, it's time we had a talk.

ow you mean well. I know you think you're helping. But
en you demand that your co-workers' passwords change

Slate

future tense ASU | NEW AMERICA | SLATE

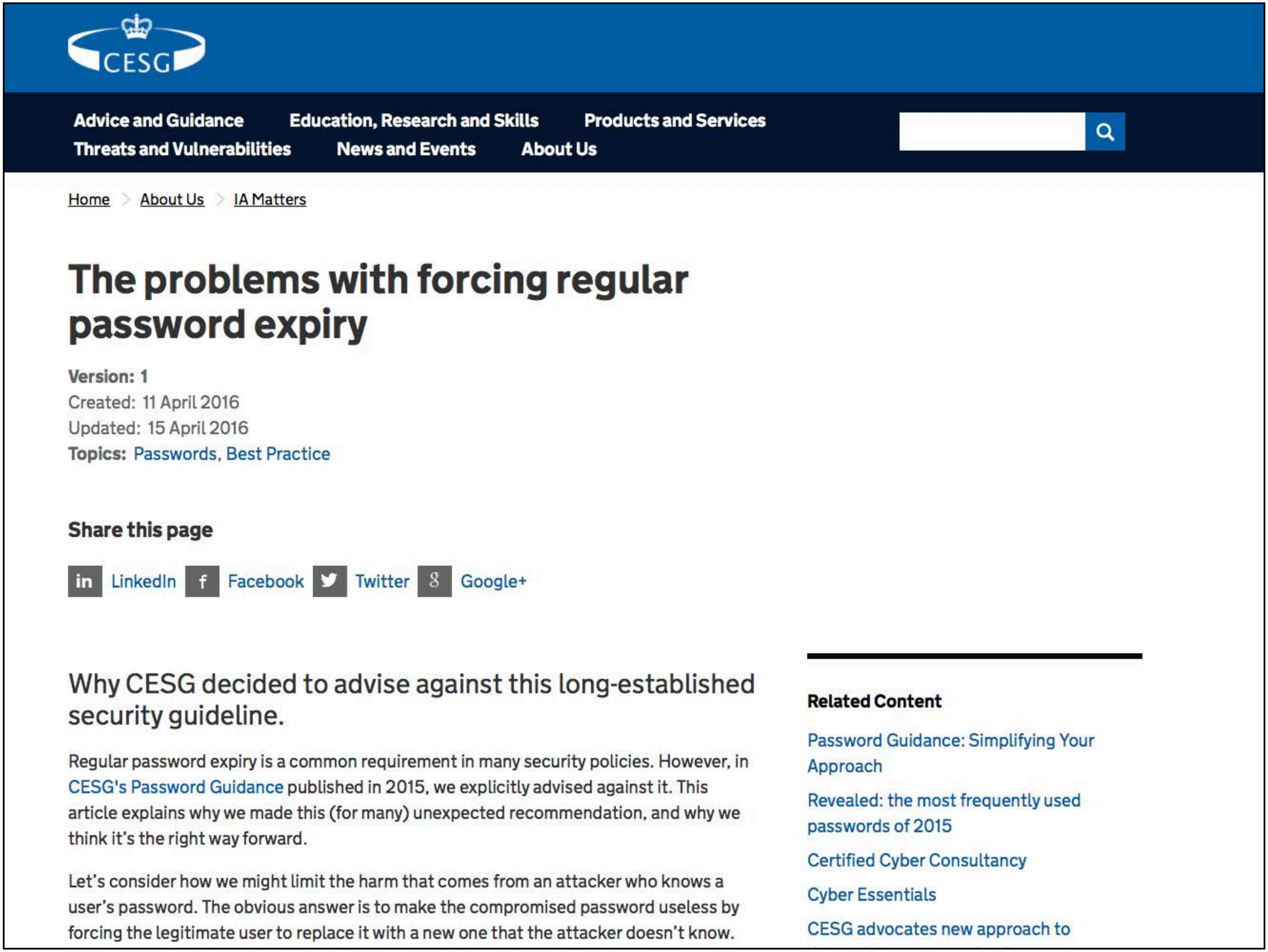
Learn more about Future Tense »

future tense THE CITIZEN'S GUIDE TO THE FUTURE MARCH 3 2016 5:10 PM

Forcing People to Change Their Passwords Isn't Just Annoying. It's Counterproductive.

By Lily Hay Newman

749 159 93



The problems with forcing regular password expiry

Version: 1
Created: 11 April 2016
Updated: 15 April 2016
Topics: Passwords, Best Practice

Share this page

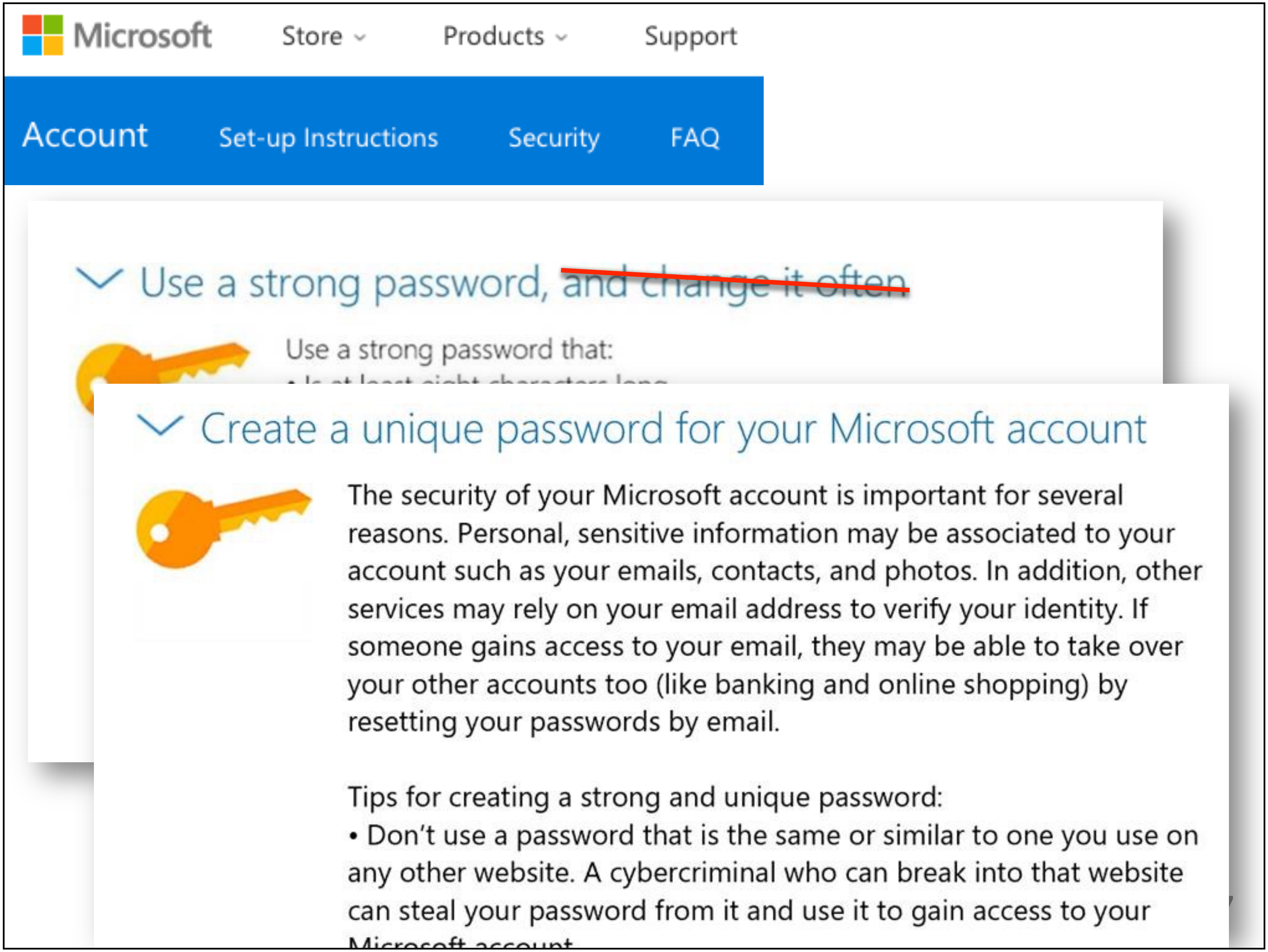
Why CESG decided to advise against this long-established security guideline.

Regular password expiry is a common requirement in many security policies. However, in CESG's Password Guidance published in 2015, we explicitly advised against it. This article explains why we made this (for many) unexpected recommendation, and why we think it's the right way forward.

Let's consider how we might limit the harm that comes from an attacker who knows a user's password. The obvious answer is to make the compromised password useless by forcing the legitimate user to replace it with a new one that the attacker doesn't know.

Related Content

- Password Guidance: Simplifying Your Approach
- Revealed: the most frequently used passwords of 2015
- Certified Cyber Consultancy
- Cyber Essentials
- CESG advocates new approach to



Use a strong password, ~~and change it often~~

Use a strong password that:

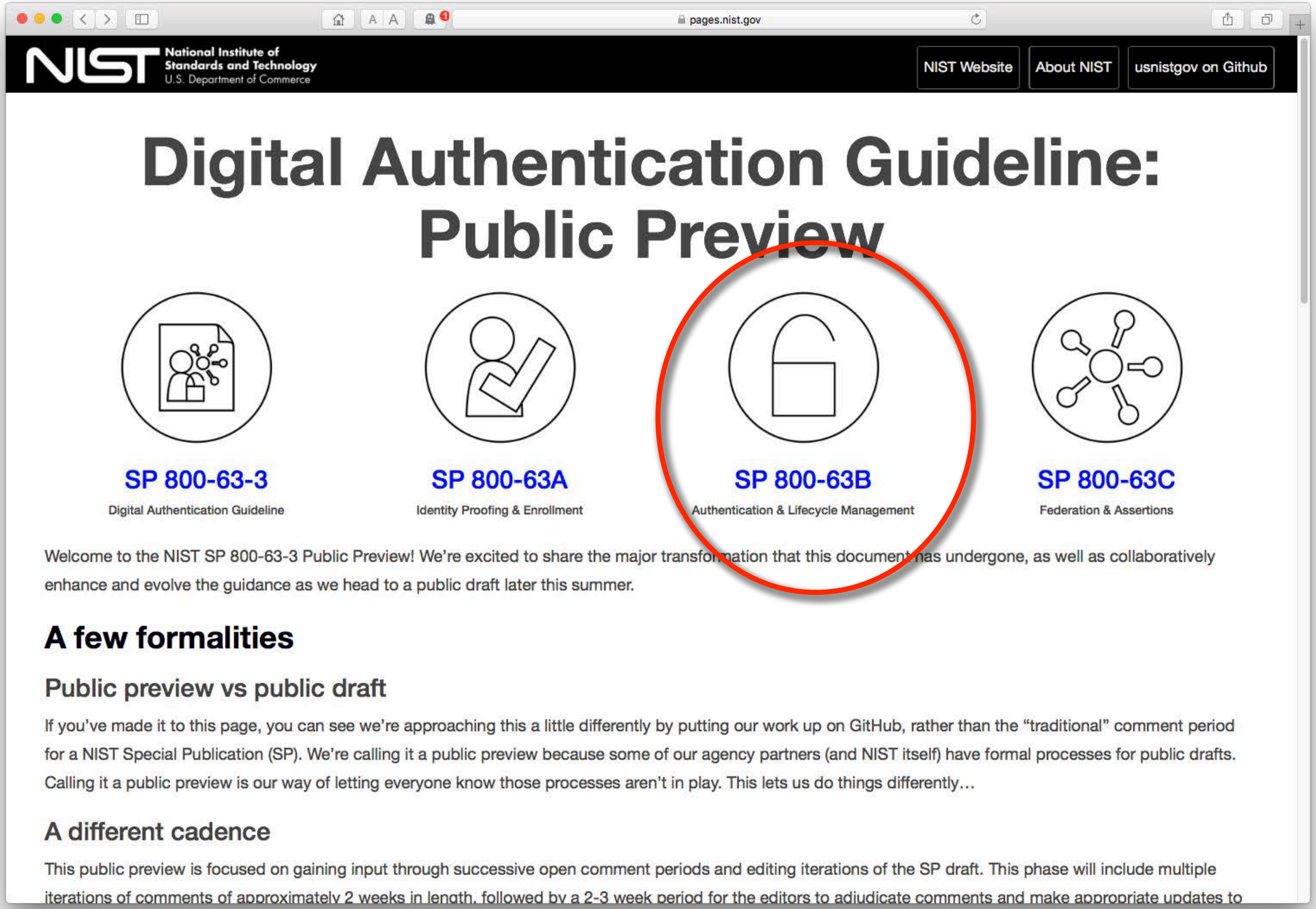
• Is at least eight characters long

Create a unique password for your Microsoft account

The security of your Microsoft account is important for several reasons. Personal, sensitive information may be associated to your account such as your emails, contacts, and photos. In addition, other services may rely on your email address to verify your identity. If someone gains access to your email, they may be able to take over your other accounts too (like banking and online shopping) by resetting your passwords by email.

Tips for creating a strong and unique password:

• Don't use a password that is the same or similar to one you use on any other website. A cybercriminal who can break into that website can steal your password from it and use it to gain access to your Microsoft account


pages.nist.gov
National Institute of Standards and Technology U.S. Department of Commerce
NIST Website
About NIST
usnistgov on Github

Digital Authentication Guideline: Public Preview

SP 800-63-3
Digital Authentication Guideline

SP 800-63A
Identity Proofing & Enrollment

SP 800-63B
Authentication & Lifecycle Management

SP 800-63C
Federation & Assertions

Welcome to the NIST SP 800-63-3 Public Preview! We're excited to share the major transformation that this document has undergone, as well as collaboratively enhance and evolve the guidance as we head to a public draft later this summer.

A few formalities

Public preview vs public draft

If you've made it to this page, you can see we're approaching this a little differently by putting our work up on GitHub, rather than the "traditional" comment period for a NIST Special Publication (SP). We're calling it a public preview because some of our agency partners (and NIST itself) have formal processes for public drafts. Calling it a public preview is our way of letting everyone know those processes aren't in play. This lets us do things differently…

A different cadence

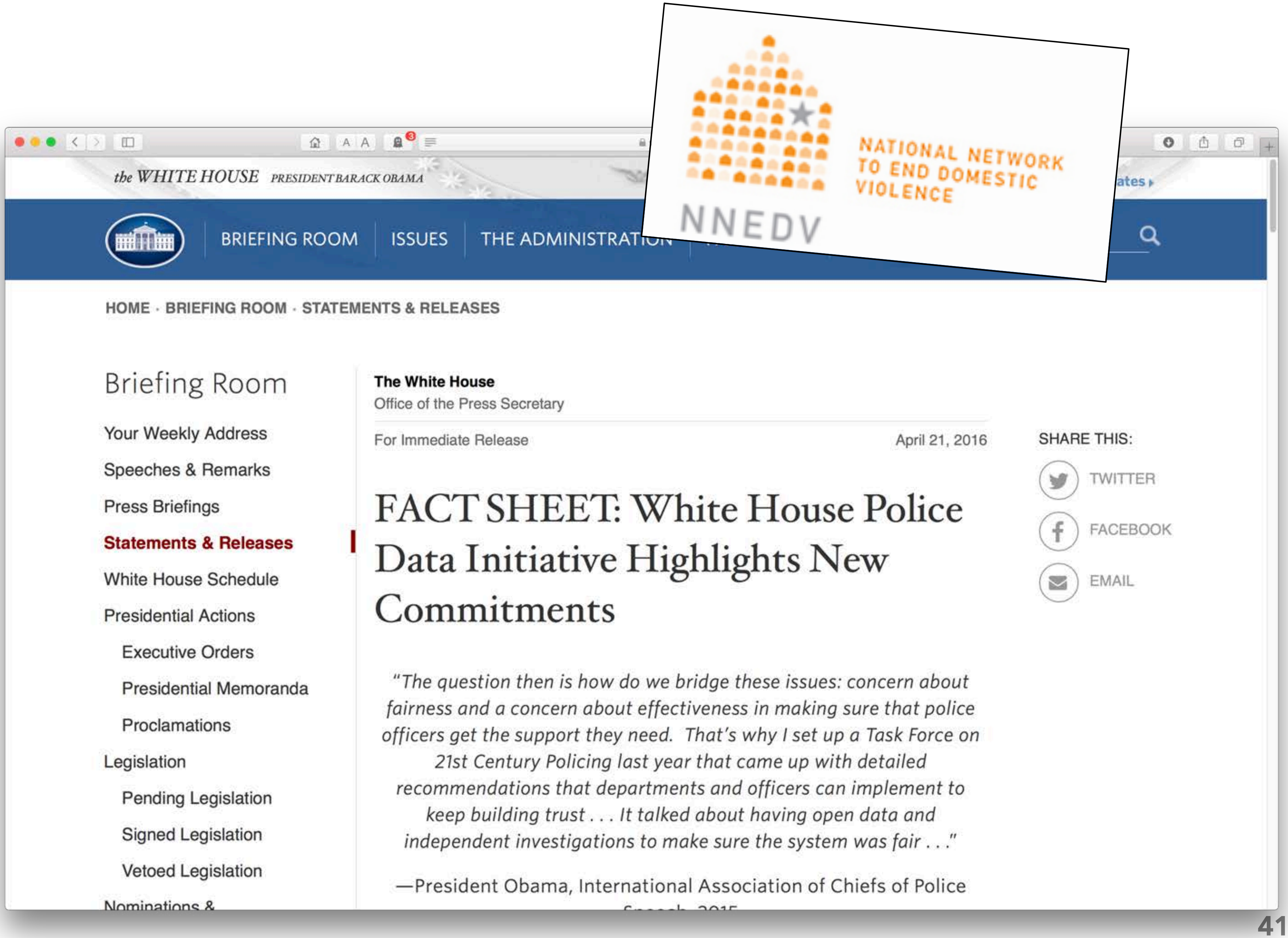
This public preview is focused on gaining input through successive open comment periods and editing iterations of the SP draft. This phase will include multiple iterations of comments of approximately 2 weeks in length, followed by a 2-3 week period for the editors to adjudicate comments and make appropriate updates to

NIST preview (comments wanted) Memorized user-chosen secrets

- >= 8 characters
- Allow at least 64 characters, all printing ASCII characters, space
- Do not truncate
- Do not store a hint
- Do not prompt for secret questions (name of first pet)
- Do not impose composition rules
- Blacklist common passwords
- Implement throttling mechanism to limit failed authentication attempts
- Do not require arbitrary periodic password change
- Offer option to display secret when typed and hide after sufficient time
- Store with salt and slow hash

https://pages.nist.gov/800-63-3/sp800-63b.html
5.1.1.2. Memorized Secret Verifiers

Open police data


NATIONAL NETWORK TO END DOMESTIC VIOLENCE
NNEDV
the WHITE HOUSE PRESIDENT BARACK OBAMA
BRIEFING ROOM
ISSUES
THE ADMINISTRATION

HOME · BRIEFING ROOM · STATEMENTS & RELEASES

Briefing Room

- Your Weekly Address
- Speeches & Remarks
- Press Briefings
- **Statements & Releases**
- White House Schedule
- Presidential Actions
  - Executive Orders
  - Presidential Memoranda
  - Proclamations
- Legislation
  - Pending Legislation
  - Signed Legislation
  - Vetoed Legislation
- Nominations &

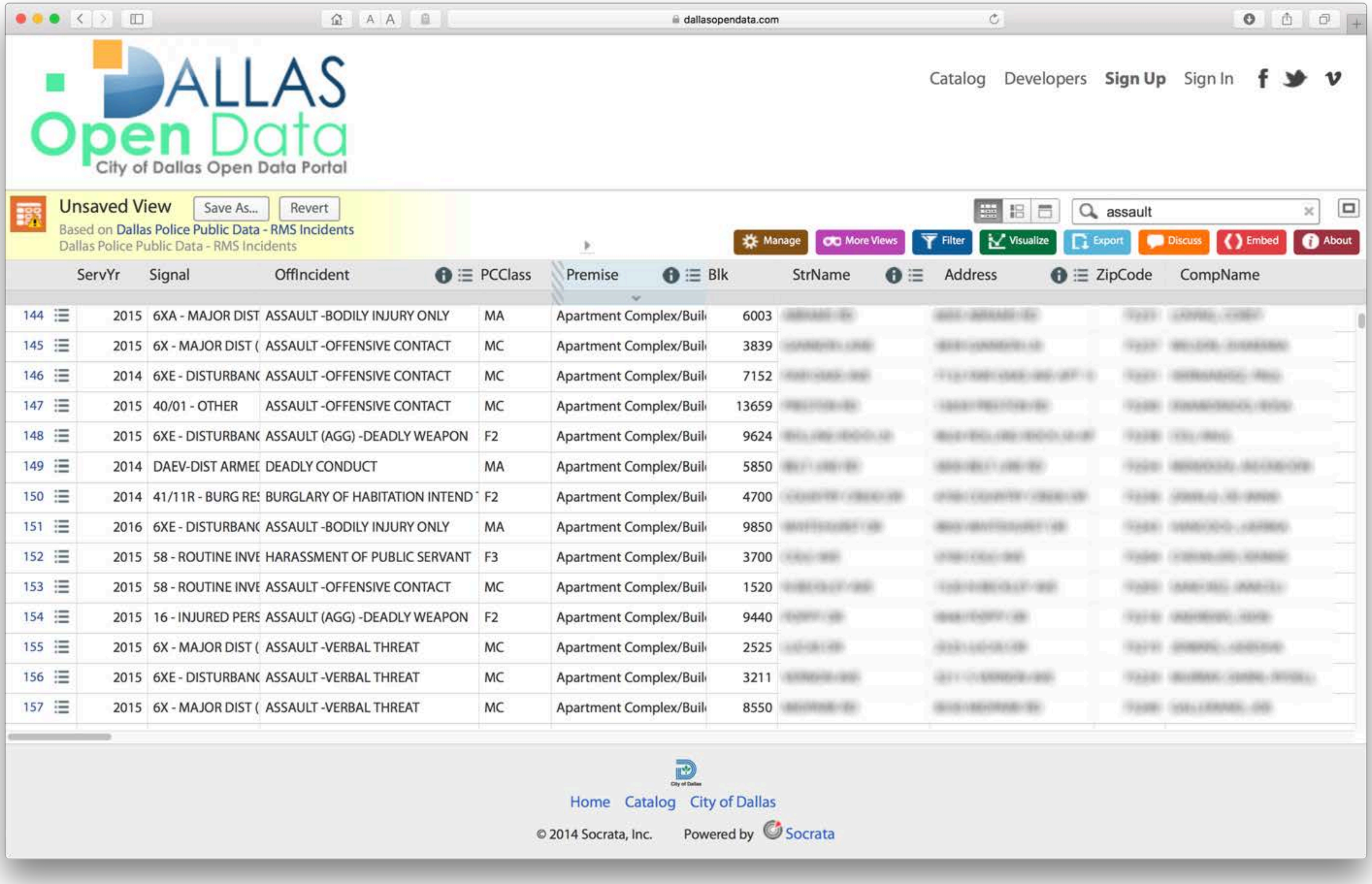
The White House
Office of the Press Secretary

For Immediate Release April 21, 2016

FACT SHEET: White House Police Data Initiative Highlights New Commitments

> *"The question then is how do we bridge these issues: concern about fairness and a concern about effectiveness in making sure that police officers get the support they need. That's why I set up a Task Force on 21st Century Policing last year that came up with detailed recommendations that departments and officers can implement to keep building trust . . . It talked about having open data and independent investigations to make sure the system was fair . . ."*
>
> —President Obama, International Association of Chiefs of Police Speech, 2015

SHARE THIS:
TWITTER
FACEBOOK
EMAIL



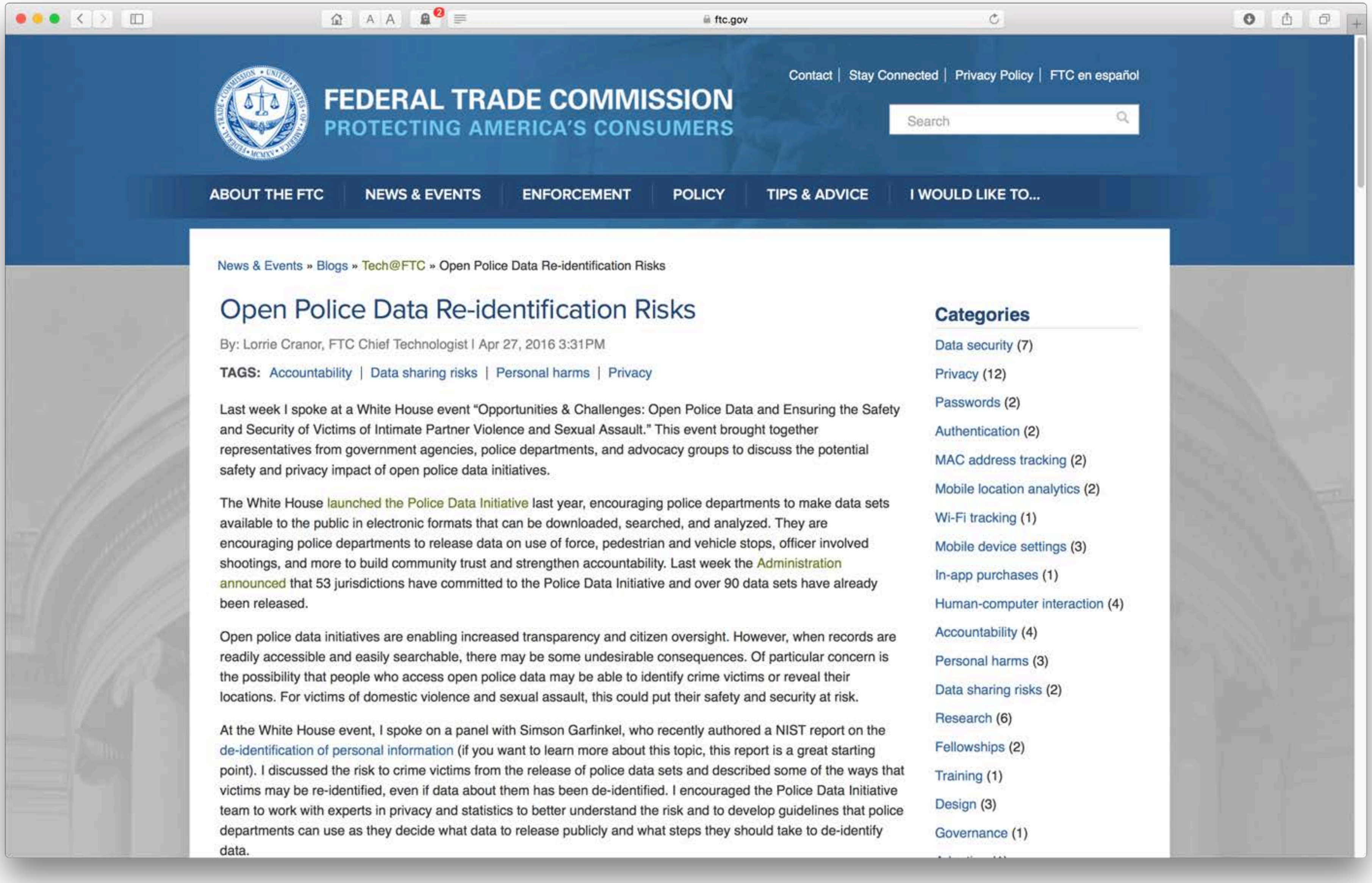
Based on Dallas Police Public Data - RMS Incidents
Dallas Police Public Data - RMS Incidents

	ServYr	Signal	OffIncident	PCClass	Premise	Blk	StrName	Address	ZipCode	CompName
144	2015	6XA - MAJOR DIST	ASSAULT -BODILY INJURY ONLY	MA	Apartment Complex/Buil	6003	[redacted]	[redacted]	[redacted]	[redacted]
145	2015	6X - MAJOR DIST (	ASSAULT -OFFENSIVE CONTACT	MC	Apartment Complex/Buil	3839	[redacted]	[redacted]	[redacted]	[redacted]
146	2014	6XE - DISTURBANC	ASSAULT -OFFENSIVE CONTACT	MC	Apartment Complex/Buil	7152	[redacted]	[redacted]	[redacted]	[redacted]
147	2015	40/01 - OTHER	ASSAULT -OFFENSIVE CONTACT	MC	Apartment Complex/Buil	13659	[redacted]	[redacted]	[redacted]	[redacted]
148	2015	6XE - DISTURBANC	ASSAULT (AGG) -DEADLY WEAPON	F2	Apartment Complex/Buil	9624	[redacted]	[redacted]	[redacted]	[redacted]
149	2014	DAEV-DIST ARMEI	DEADLY CONDUCT	MA	Apartment Complex/Buil	5850	[redacted]	[redacted]	[redacted]	[redacted]
150	2014	41/11R - BURG RES	BURGLARY OF HABITATION INTEND	F2	Apartment Complex/Buil	4700	[redacted]	[redacted]	[redacted]	[redacted]
151	2016	6XE - DISTURBANC	ASSAULT -BODILY INJURY ONLY	MA	Apartment Complex/Buil	9850	[redacted]	[redacted]	[redacted]	[redacted]
152	2015	58 - ROUTINE INVE	HARASSMENT OF PUBLIC SERVANT	F3	Apartment Complex/Buil	3700	[redacted]	[redacted]	[redacted]	[redacted]
153	2015	58 - ROUTINE INVE	ASSAULT -OFFENSIVE CONTACT	MC	Apartment Complex/Buil	1520	[redacted]	[redacted]	[redacted]	[redacted]
154	2015	16 - INJURED PERS	ASSAULT (AGG) -DEADLY WEAPON	F2	Apartment Complex/Buil	9440	[redacted]	[redacted]	[redacted]	[redacted]
155	2015	6X - MAJOR DIST (	ASSAULT -VERBAL THREAT	MC	Apartment Complex/Buil	2525	[redacted]	[redacted]	[redacted]	[redacted]
156	2015	6XE - DISTURBANC	ASSAULT -VERBAL THREAT	MC	Apartment Complex/Buil	3211	[redacted]	[redacted]	[redacted]	[redacted]
157	2015	6X - MAJOR DIST (	ASSAULT -VERBAL THREAT	MC	Apartment Complex/Buil	8550	[redacted]	[redacted]	[redacted]	[redacted]

Home Catalog City of Dallas

© 2014 Socrata, Inc. Powered by Socrata

EXIT
Austin
Rose
Rosie Hidalgo
Senior Policy Advisor
Office on Violence Against Women
Department of Justice



News & Events » Blogs » Tech@FTC » Open Police Data Re-identification Risks

Open Police Data Re-identification Risks

By: Lorrie Cranor, FTC Chief Technologist | Apr 27, 2016 3:31PM

TAGS: Accountability | Data sharing risks | Personal harms | Privacy

Last week I spoke at a White House event "Opportunities & Challenges: Open Police Data and Ensuring the Safety and Security of Victims of Intimate Partner Violence and Sexual Assault." This event brought together representatives from government agencies, police departments, and advocacy groups to discuss the potential safety and privacy impact of open police data initiatives.

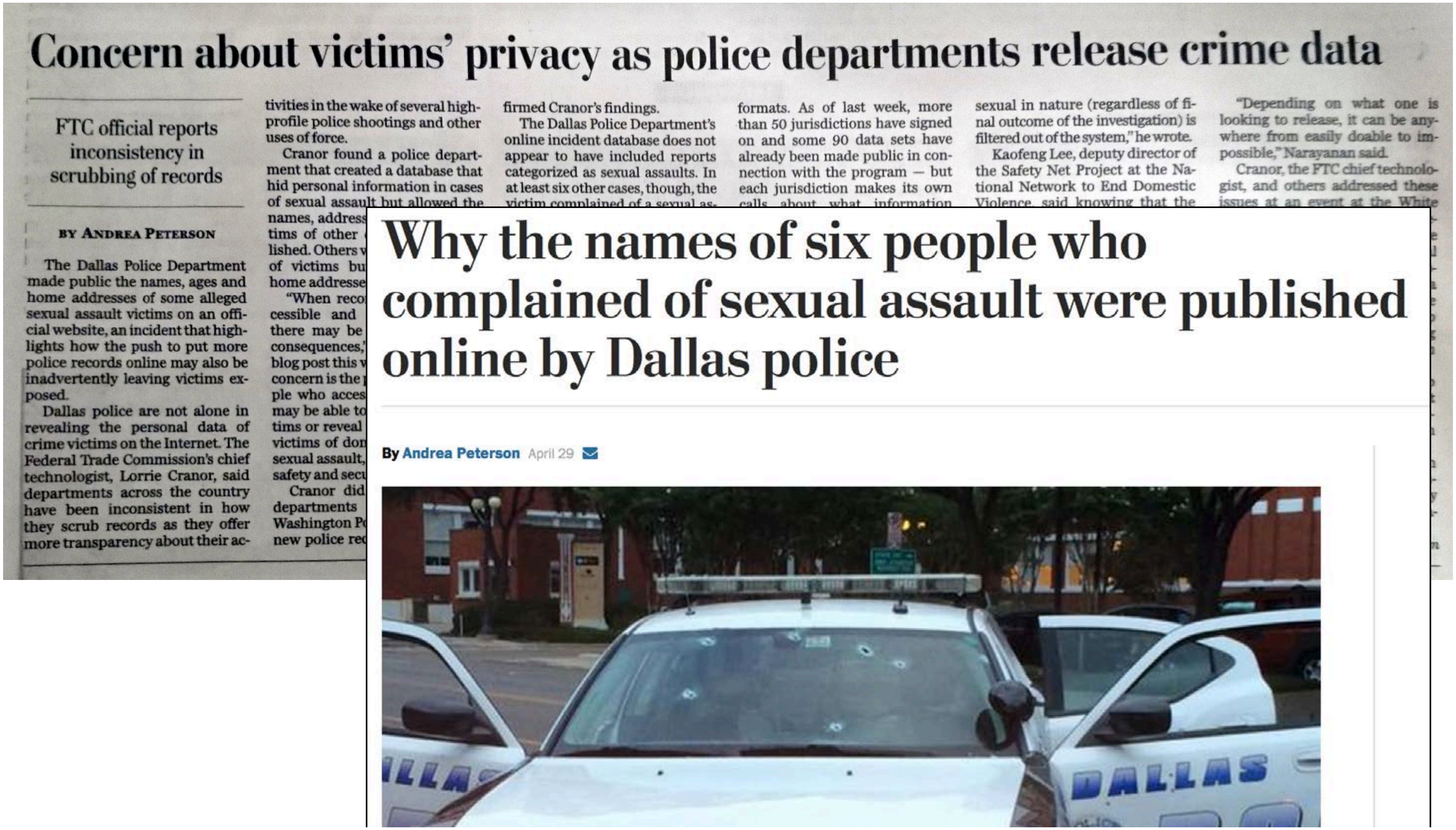
The White House launched the Police Data Initiative last year, encouraging police departments to make data sets available to the public in electronic formats that can be downloaded, searched, and analyzed. They are encouraging police departments to release data on use of force, pedestrian and vehicle stops, officer involved shootings, and more to build community trust and strengthen accountability. Last week the Administration announced that 53 jurisdictions have committed to the Police Data Initiative and over 90 data sets have already been released.

Open police data initiatives are enabling increased transparency and citizen oversight. However, when records are readily accessible and easily searchable, there may be some undesirable consequences. Of particular concern is the possibility that people who access open police data may be able to identify crime victims or reveal their locations. For victims of domestic violence and sexual assault, this could put their safety and security at risk.

At the White House event, I spoke on a panel with Simson Garfinkel, who recently authored a NIST report on the de-identification of personal information (if you want to learn more about this topic, this report is a great starting point). I discussed the risk to crime victims from the release of police data sets and described some of the ways that victims may be re-identified, even if data about them has been de-identified. I encouraged the Police Data Initiative team to work with experts in privacy and statistics to better understand the risk and to develop guidelines that police departments can use as they decide what data to release publicly and what steps they should take to de-identify data.

Categories

- Data security (7)
- Privacy (12)
- Passwords (2)
- Authentication (2)
- MAC address tracking (2)
- Mobile location analytics (2)
- Wi-Fi tracking (1)
- Mobile device settings (3)
- In-app purchases (1)
- Human-computer interaction (4)
- Accountability (4)
- Personal harms (3)
- Data sharing risks (2)
- Research (6)
- Fellowships (2)
- Training (1)
- Design (3)
- Governance (1)



Concern about victims' privacy as police departments release crime data

FTC official reports inconsistency in scrubbing of records

BY ANDREA PETERSON

The Dallas Police Department made public the names, ages and home addresses of some alleged sexual assault victims on an official website, an incident that highlights how the push to put more police records online may also be inadvertently leaving victims exposed.

Dallas police are not alone in revealing the personal data of crime victims on the Internet. The Federal Trade Commission's chief technologist, Lorrie Cranor, said departments across the country have been inconsistent in how they scrub records as they offer more transparency about their activities in the wake of several high-profile police shootings and other uses of force.

Cranor found a police department that created a database that hid personal information in cases of sexual assault but allowed the
names, address
tims of other
lished. Others w
of victims bu
home addresse
"When reco
cessible and
there may be
consequences,'
blog post this w
concern is the p
ple who acces
may be able to
tims or reveal
victims of dom
sexual assault,
safety and secu
Cranor did
departments
Washington Po
new police rec

firmed Cranor's findings.

The Dallas Police Department's online incident database does not appear to have included reports categorized as sexual assaults. In at least six other cases, though, the victim complained of a sexual as-

formats. As of last week, more than 50 jurisdictions have signed on and some 90 data sets have already been made public in connection with the program — but each jurisdiction makes its own calls about what information

sexual in nature (regardless of final outcome of the investigation) is filtered out of the system," he wrote.

Kaofeng Lee, deputy director of the Safety Net Project at the National Network to End Domestic Violence, said knowing that the

"Depending on what one is looking to release, it can be anywhere from easily doable to impossible," Narayanan said.

Cranor, the FTC chief technologist, and others addressed these issues at an event at the White

Why the names of six people who complained of sexual assault were published online by Dallas police

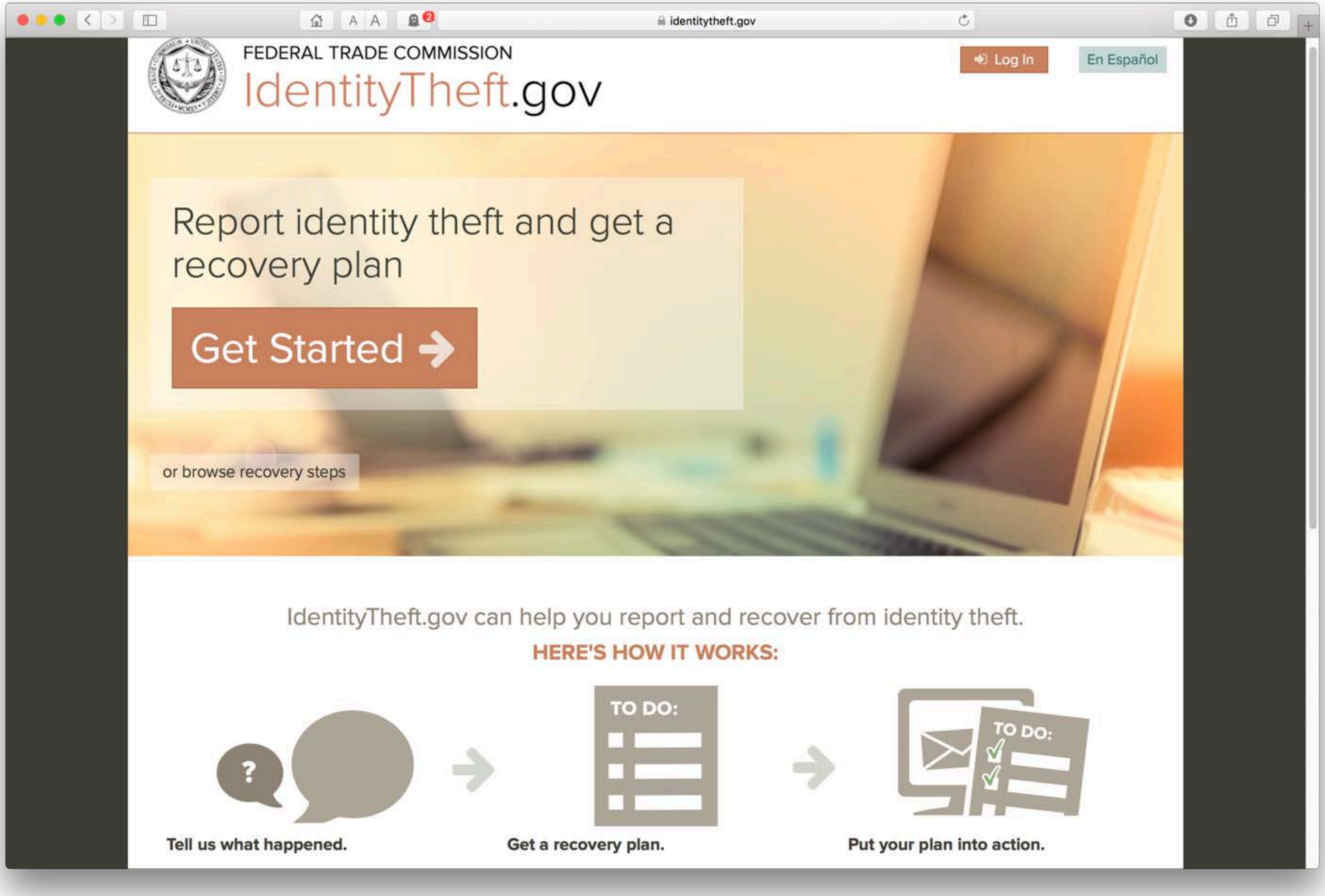
By Andrea Peterson April 29

This story has been updated with a statement from the Dallas Police Department, saying it plans to remove the six cases identified by The Washington Post from its online database.

Phone hijacking

norman childs
eyewear
by
eyetique
iPod touch
iPhone 4S
Introducing Siri. Your wish is its command.
iOS 5
norman

FRAUD
FRAUD



Report identity theft and get a recovery plan

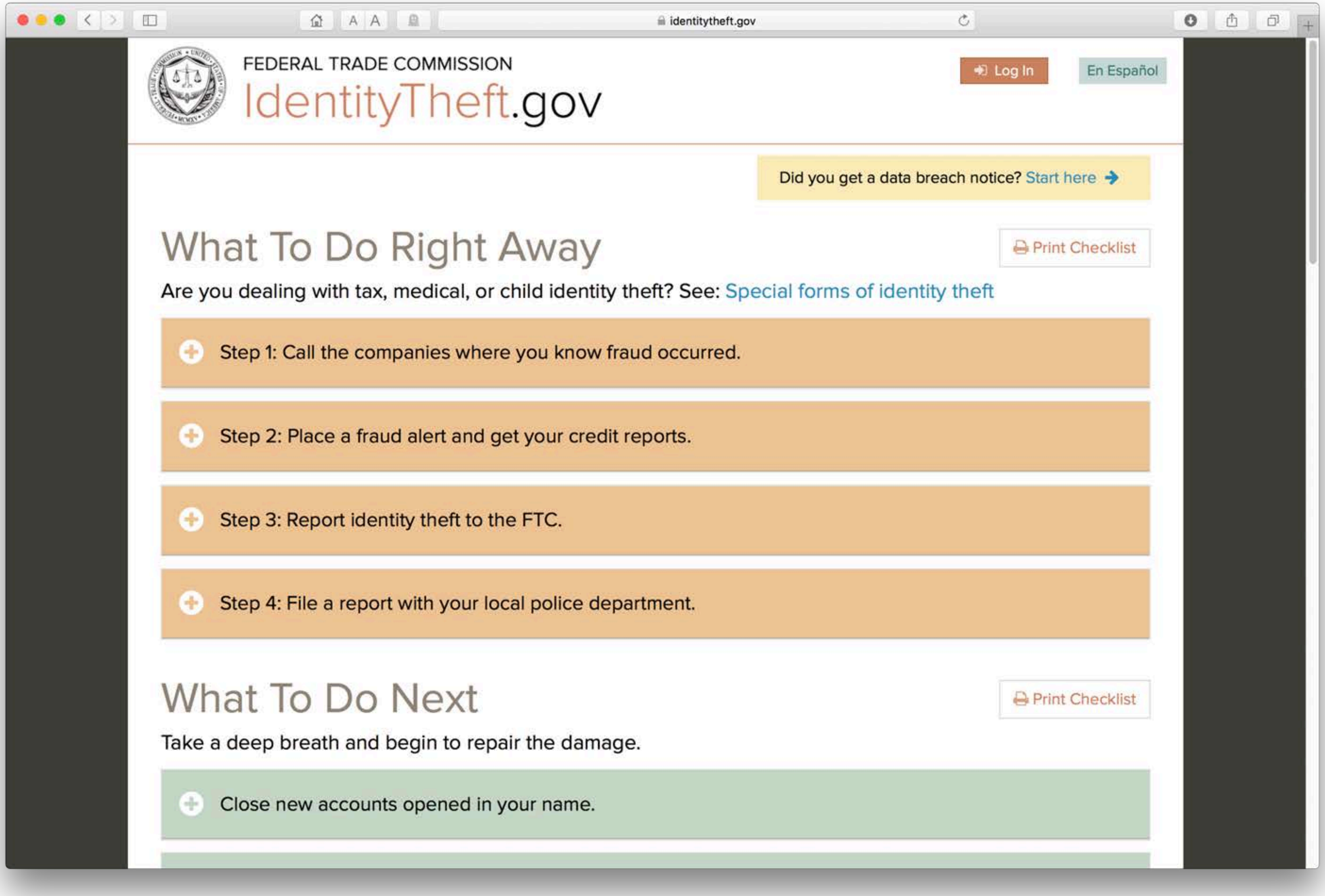
IdentityTheft.gov can help you report and recover from identity theft.

HERE'S HOW IT WORKS:

Tell us what happened.

Get a recovery plan.

Put your plan into action.



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Did you get a data breach notice? Start here

What To Do Right Away

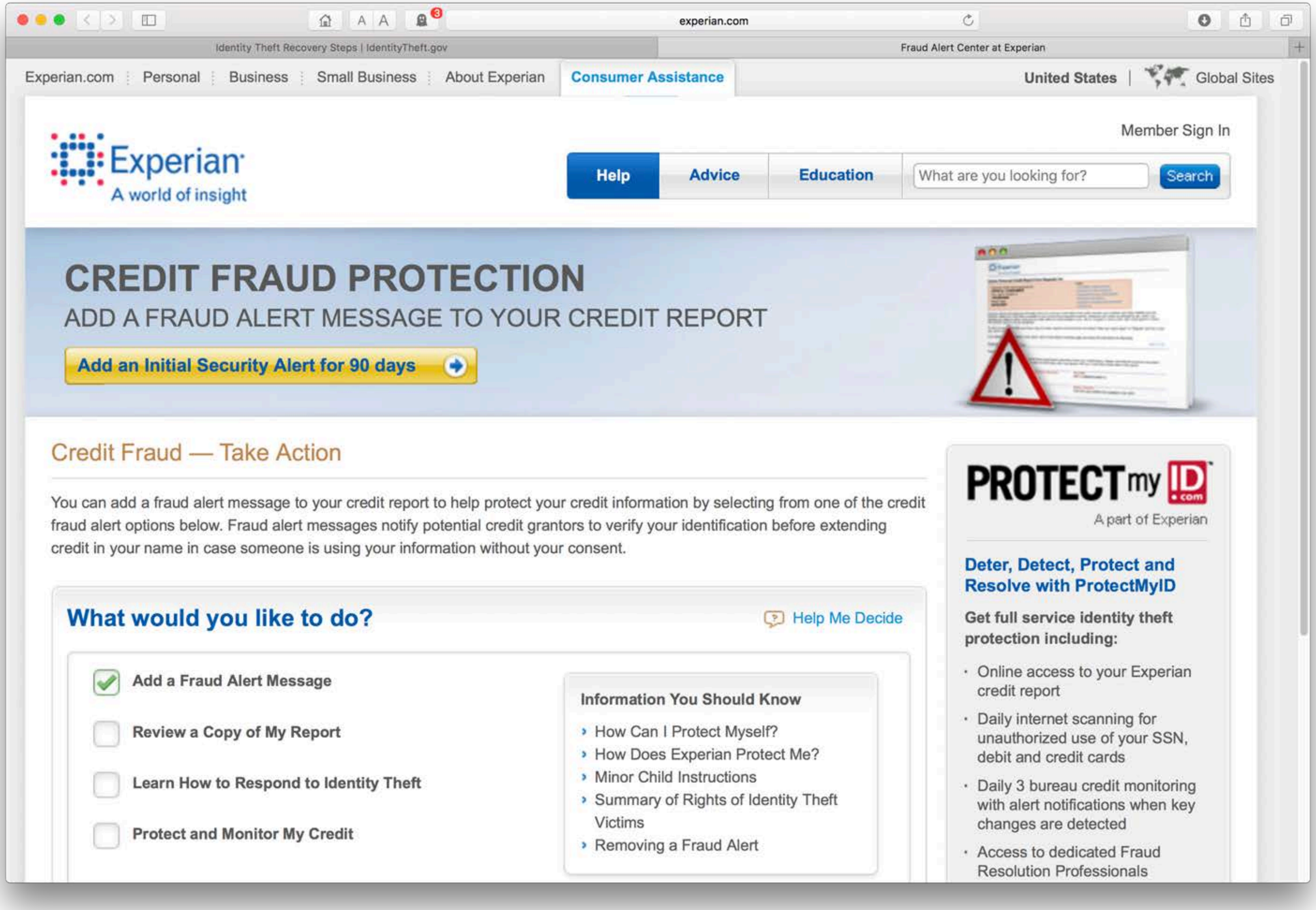
Are you dealing with tax, medical, or child identity theft? See: Special forms of identity theft

- Step 1: Call the companies where you know fraud occurred.
- Step 2: Place a fraud alert and get your credit reports.
- Step 3: Report identity theft to the FTC.
- Step 4: File a report with your local police department.

What To Do Next

Take a deep breath and begin to repair the damage.

- Close new accounts opened in your name.



CREDIT FRAUD PROTECTION

ADD A FRAUD ALERT MESSAGE TO YOUR CREDIT REPORT

Add an Initial Security Alert for 90 days

Credit Fraud — Take Action

You can add a fraud alert message to your credit report to help protect your credit information by selecting from one of the credit fraud alert options below. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent.

What would you like to do?

Help Me Decide

- ☑ Add a Fraud Alert Message
- □ Review a Copy of My Report
- □ Learn How to Respond to Identity Theft
- □ Protect and Monitor My Credit

Information You Should Know

- › How Can I Protect Myself?
- › How Does Experian Protect Me?
- › Minor Child Instructions
- › Summary of Rights of Identity Theft Victims
- › Removing a Fraud Alert

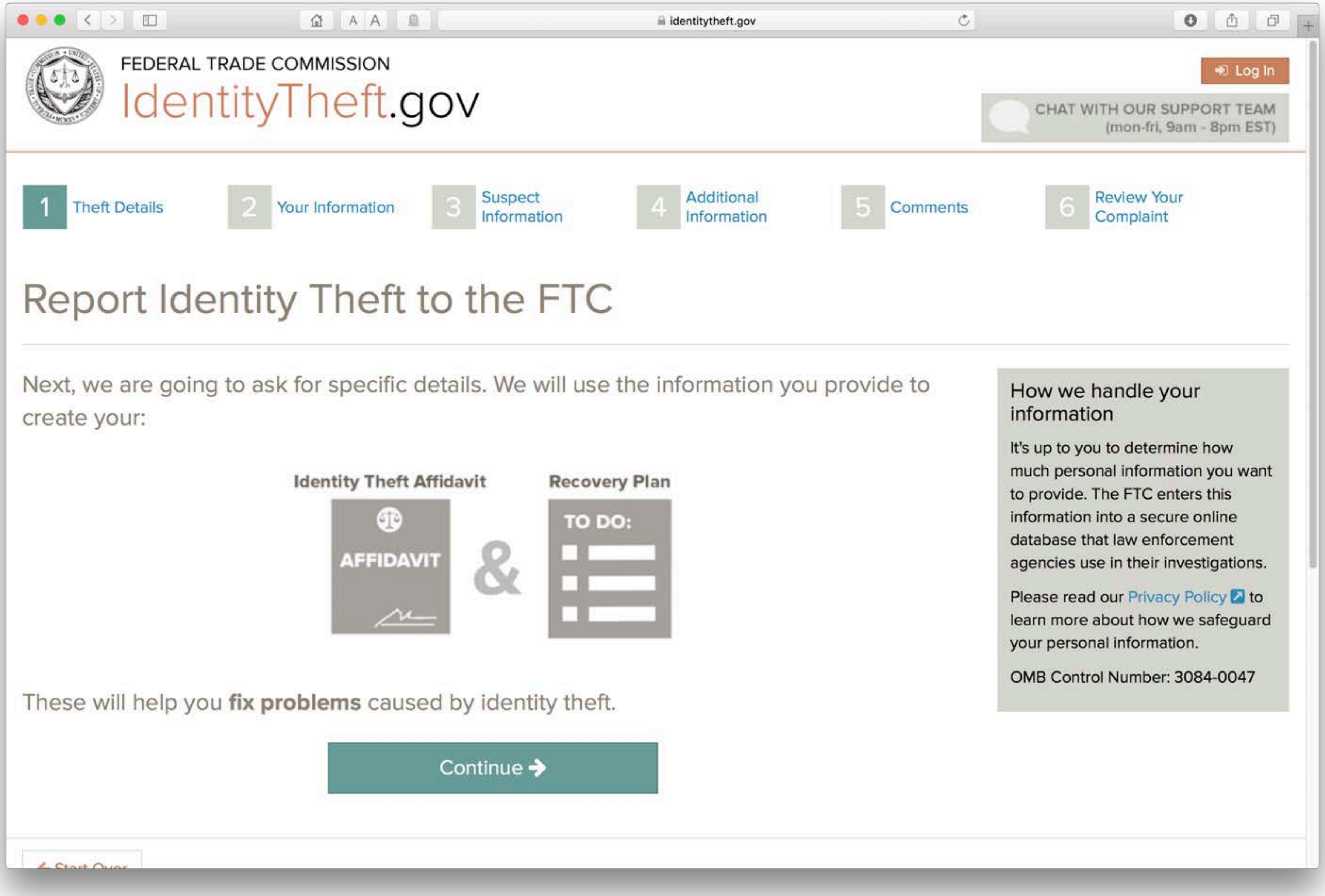
PROTECTmyID.com

A part of Experian

Deter, Detect, Protect and Resolve with ProtectMyID

Get full service identity theft protection including:

- Online access to your Experian credit report
- Daily internet scanning for unauthorized use of your SSN, debit and credit cards
- Daily 3 bureau credit monitoring with alert notifications when key changes are detected
- Access to dedicated Fraud Resolution Professionals



FEDERAL TRADE COMMISSION

IdentityTheft.gov

Report Identity Theft to the FTC

Next, we are going to ask for specific details. We will use the information you provide to create your:

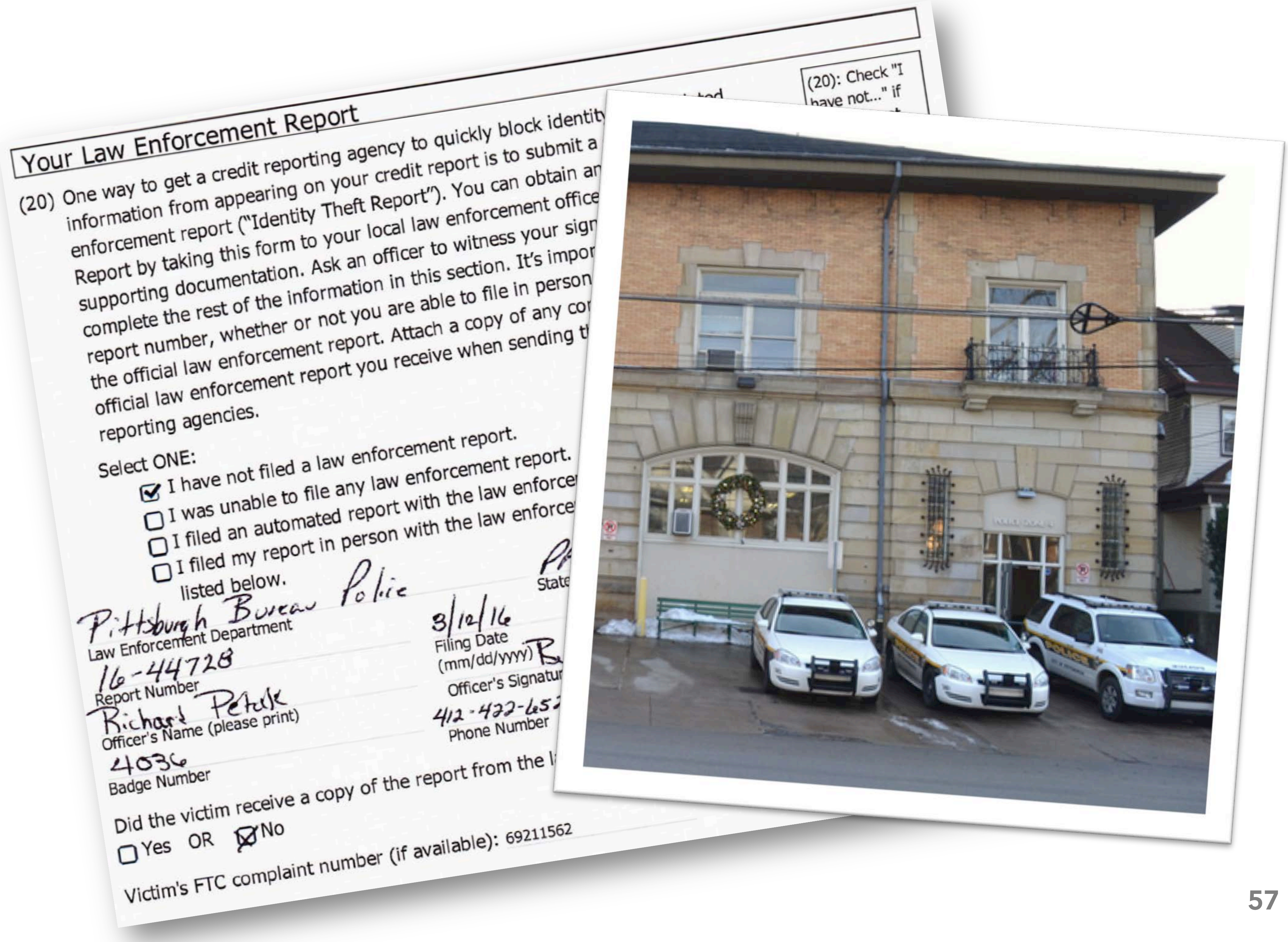
These will help you **fix problems** caused by identity theft.

How we handle your information

It's up to you to determine how much personal information you want to provide. The FTC enters this information into a secure online database that law enforcement agencies use in their investigations.

Please read our Privacy Policy to learn more about how we safeguard your personal information.

OMB Control Number: 3084-0047



Your Law Enforcement Report

(20): Check "I
have not..." if

(20) One way to get a credit reporting agency to quickly block identity
information from appearing on your credit report is to submit a
enforcement report ("Identity Theft Report"). You can obtain an
Report by taking this form to your local law enforcement office
supporting documentation. Ask an officer to witness your sign
complete the rest of the information in this section. It's impor
report number, whether or not you are able to file in person
the official law enforcement report. Attach a copy of any co
official law enforcement report you receive when sending th
reporting agencies.

Select ONE:

☑ I have not filed a law enforcement report.
□ I was unable to file any law enforcement report.
□ I filed an automated report with the law enforce
□ I filed my report in person with the law enforce
listed below.

Pittsburgh Bureau Police
Law Enforcement Department

3/12/16
Filing Date
(mm/dd/yyyy)

State

16-44728
Report Number

Officer's Signatur

Richard Petek
Officer's Name (please print)

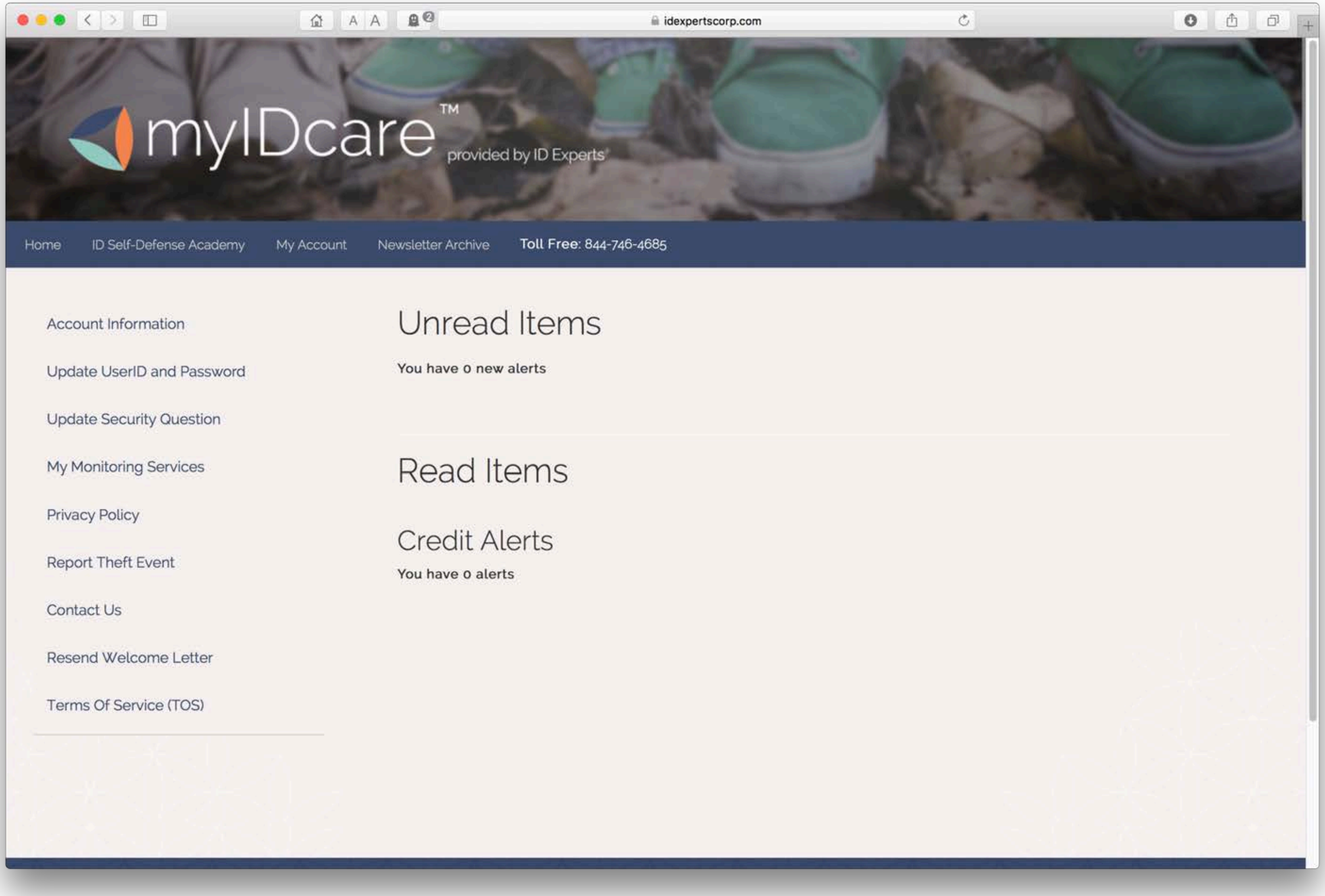
412-422-65
Phone Number

4036
Badge Number

Did the victim receive a copy of the report from the l

□ Yes OR ☒ No

Victim's FTC complaint number (if available): 69211562



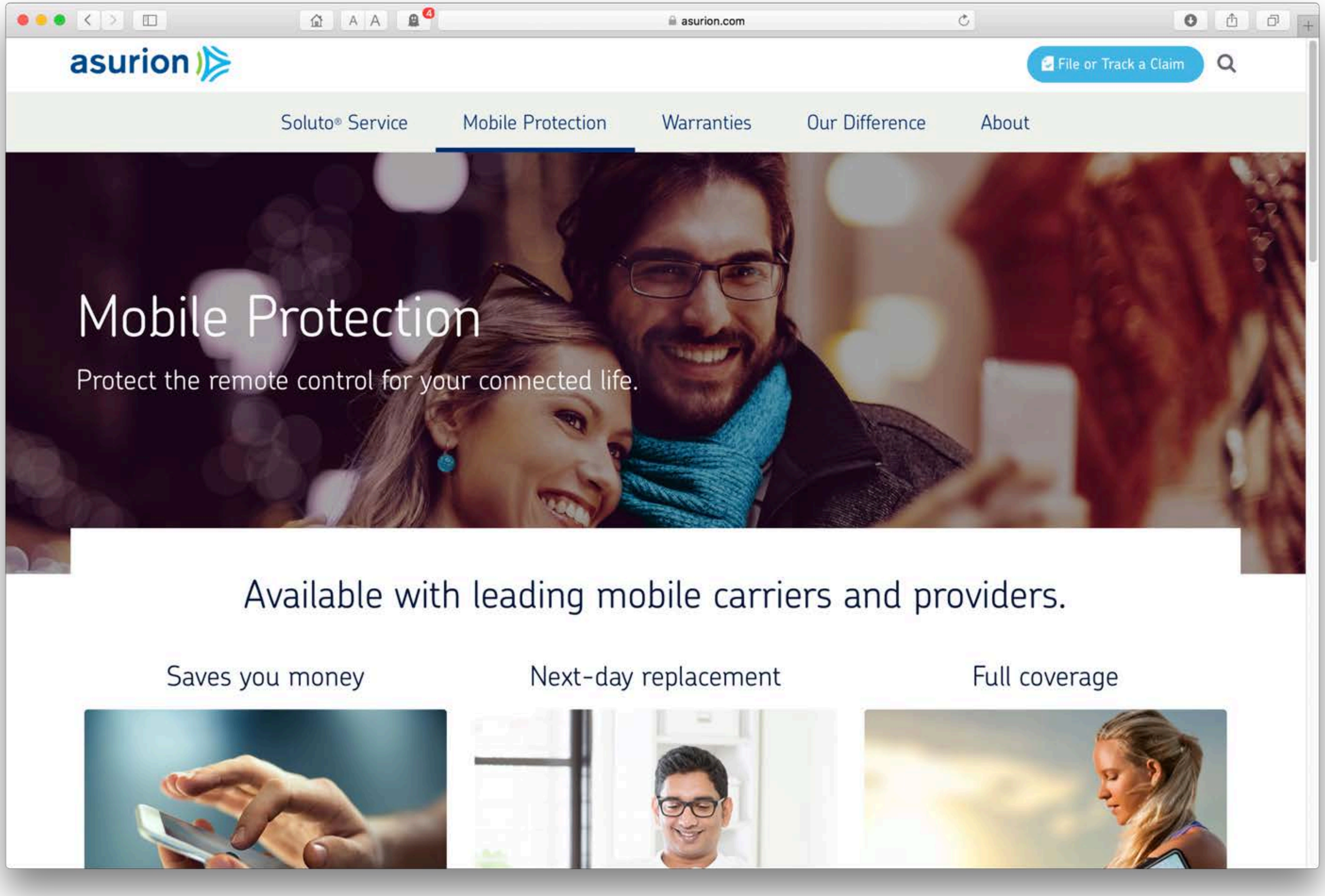
Unread Items

You have 0 new alerts

Read Items

Credit Alerts

You have 0 alerts



Mobile Protection

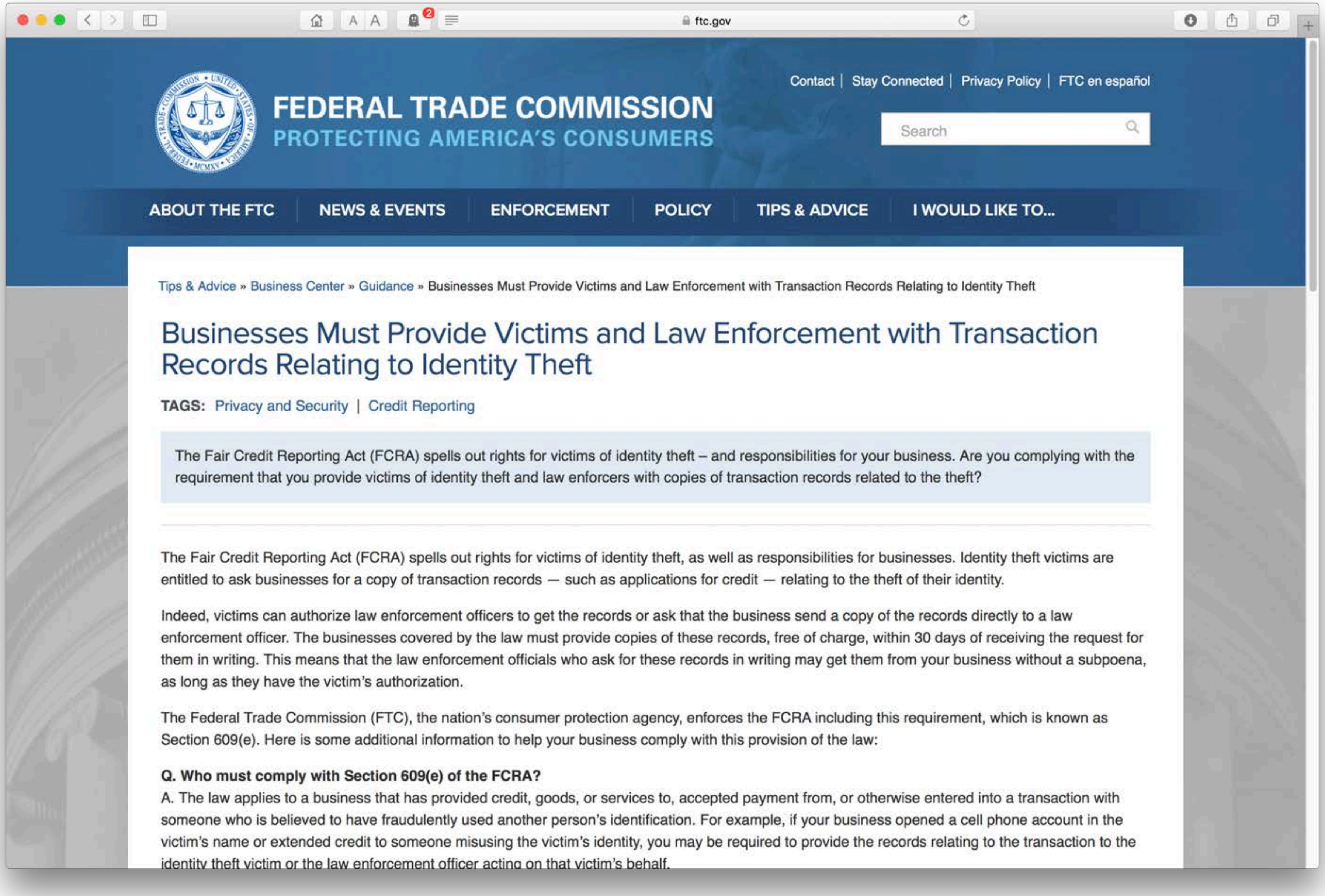
Protect the remote control for your connected life.

Available with leading mobile carriers and providers.

Saves you money

Next-day replacement

Full coverage



Tips & Advice » Business Center » Guidance » Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft

Businesses Must Provide Victims and Law Enforcement with Transaction Records Relating to Identity Theft

TAGS: Privacy and Security | Credit Reporting

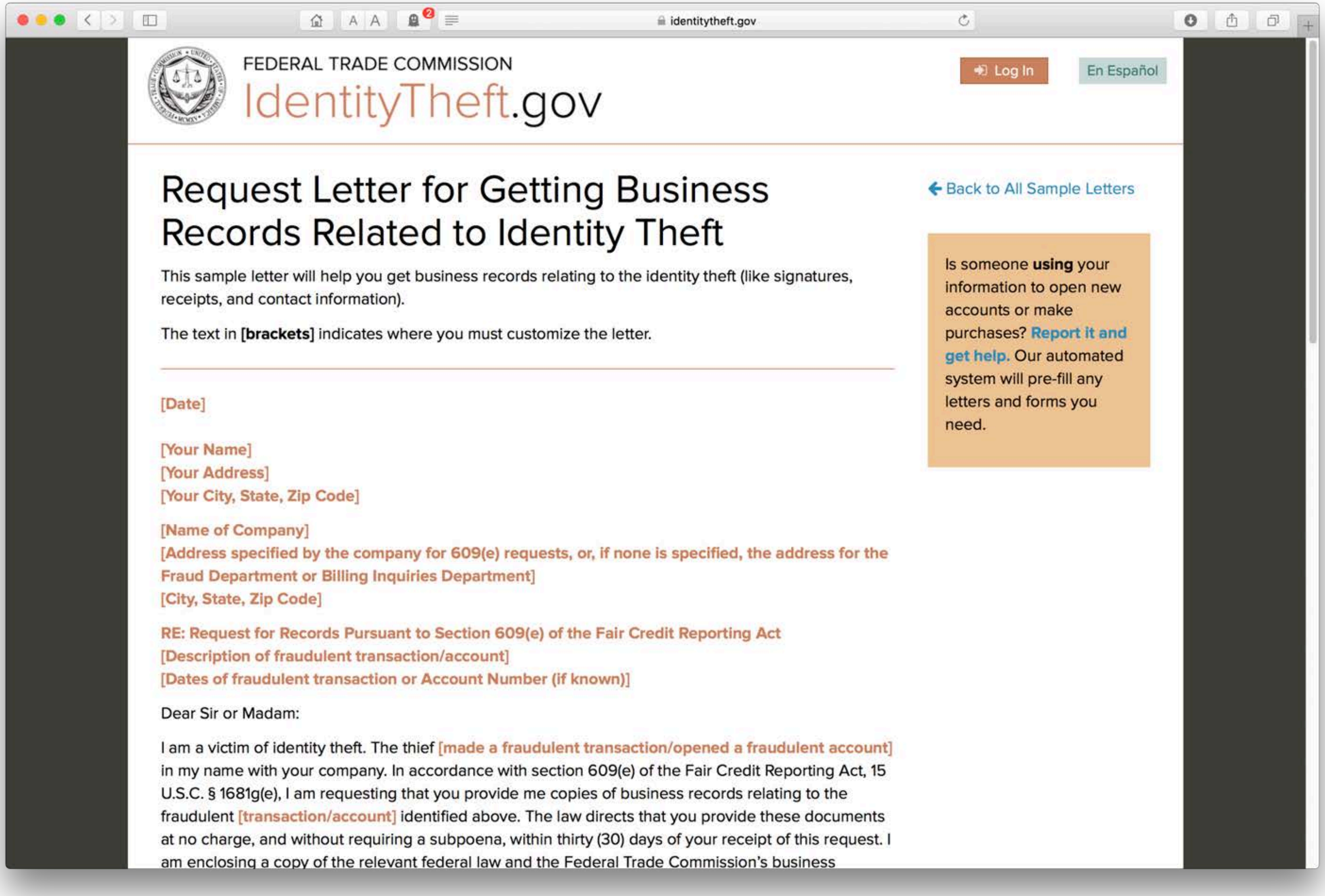
The Fair Credit Reporting Act (FCRA) spells out rights for victims of identity theft – and responsibilities for your business. Are you complying with the requirement that you provide victims of identity theft and law enforcers with copies of transaction records related to the theft?

The Fair Credit Reporting Act (FCRA) spells out rights for victims of identity theft, as well as responsibilities for businesses. Identity theft victims are entitled to ask businesses for a copy of transaction records — such as applications for credit — relating to the theft of their identity.

Indeed, victims can authorize law enforcement officers to get the records or ask that the business send a copy of the records directly to a law enforcement officer. The businesses covered by the law must provide copies of these records, free of charge, within 30 days of receiving the request for them in writing. This means that the law enforcement officials who ask for these records in writing may get them from your business without a subpoena, as long as they have the victim's authorization.

The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces the FCRA including this requirement, which is known as Section 609(e). Here is some additional information to help your business comply with this provision of the law:

Q. Who must comply with Section 609(e) of the FCRA?
A. The law applies to a business that has provided credit, goods, or services to, accepted payment from, or otherwise entered into a transaction with someone who is believed to have fraudulently used another person's identification. For example, if your business opened a cell phone account in the victim's name or extended credit to someone misusing the victim's identity, you may be required to provide the records relating to the transaction to the identity theft victim or the law enforcement officer acting on that victim's behalf.



Request Letter for Getting Business Records Related to Identity Theft

← Back to All Sample Letters

This sample letter will help you get business records relating to the identity theft (like signatures, receipts, and contact information).

The text in **[brackets]** indicates where you must customize the letter.

Is someone **using** your information to open new accounts or make purchases? **Report it and get help.** Our automated system will pre-fill any letters and forms you need.

[Date]

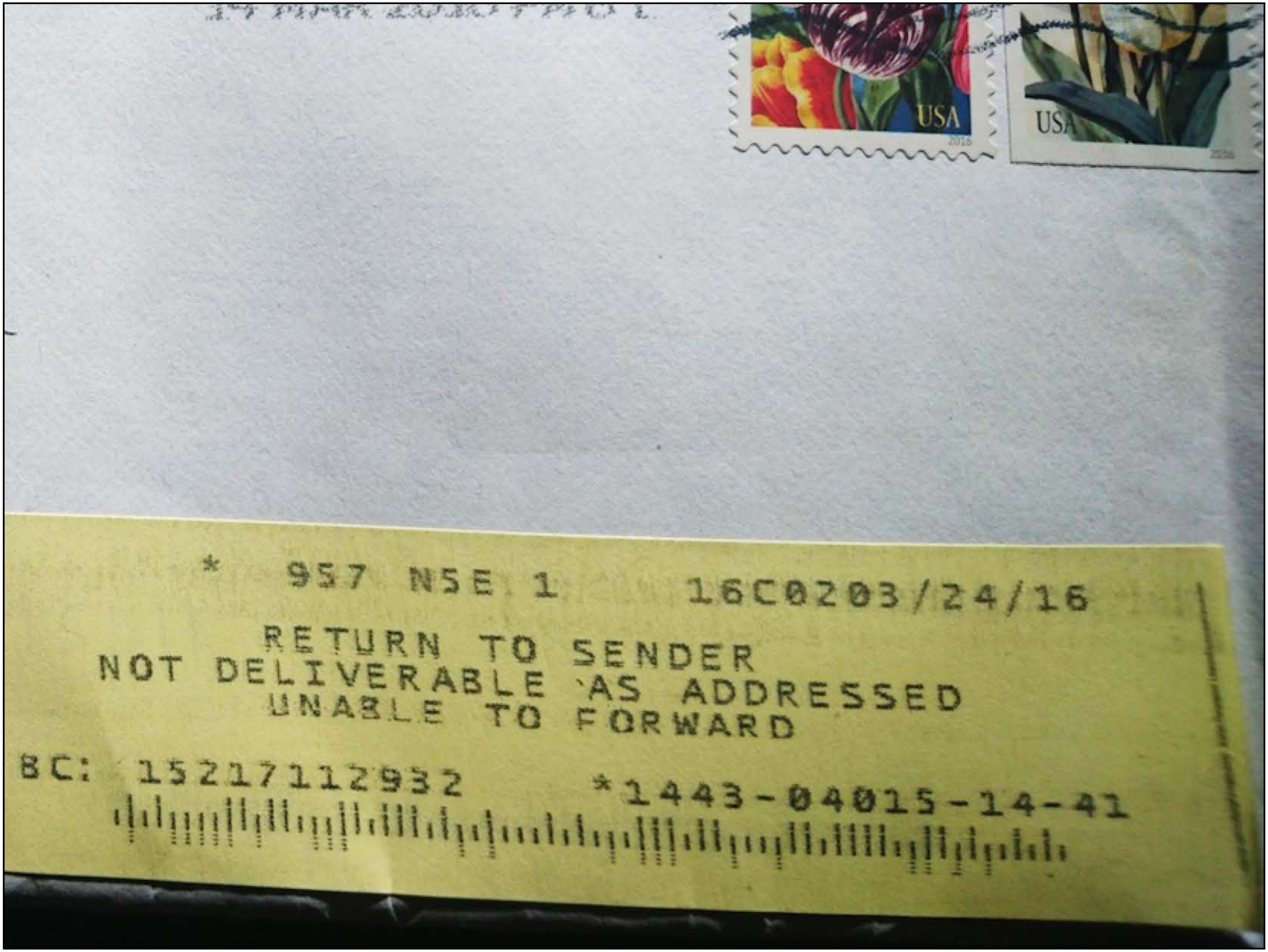
[Your Name]
[Your Address]
[Your City, State, Zip Code]

[Name of Company]
[Address specified by the company for 609(e) requests, or, if none is specified, the address for the Fraud Department or Billing Inquiries Department]
[City, State, Zip Code]

RE: Request for Records Pursuant to Section 609(e) of the Fair Credit Reporting Act
[Description of fraudulent transaction/account]
[Dates of fraudulent transaction or Account Number (if known)]

Dear Sir or Madam:

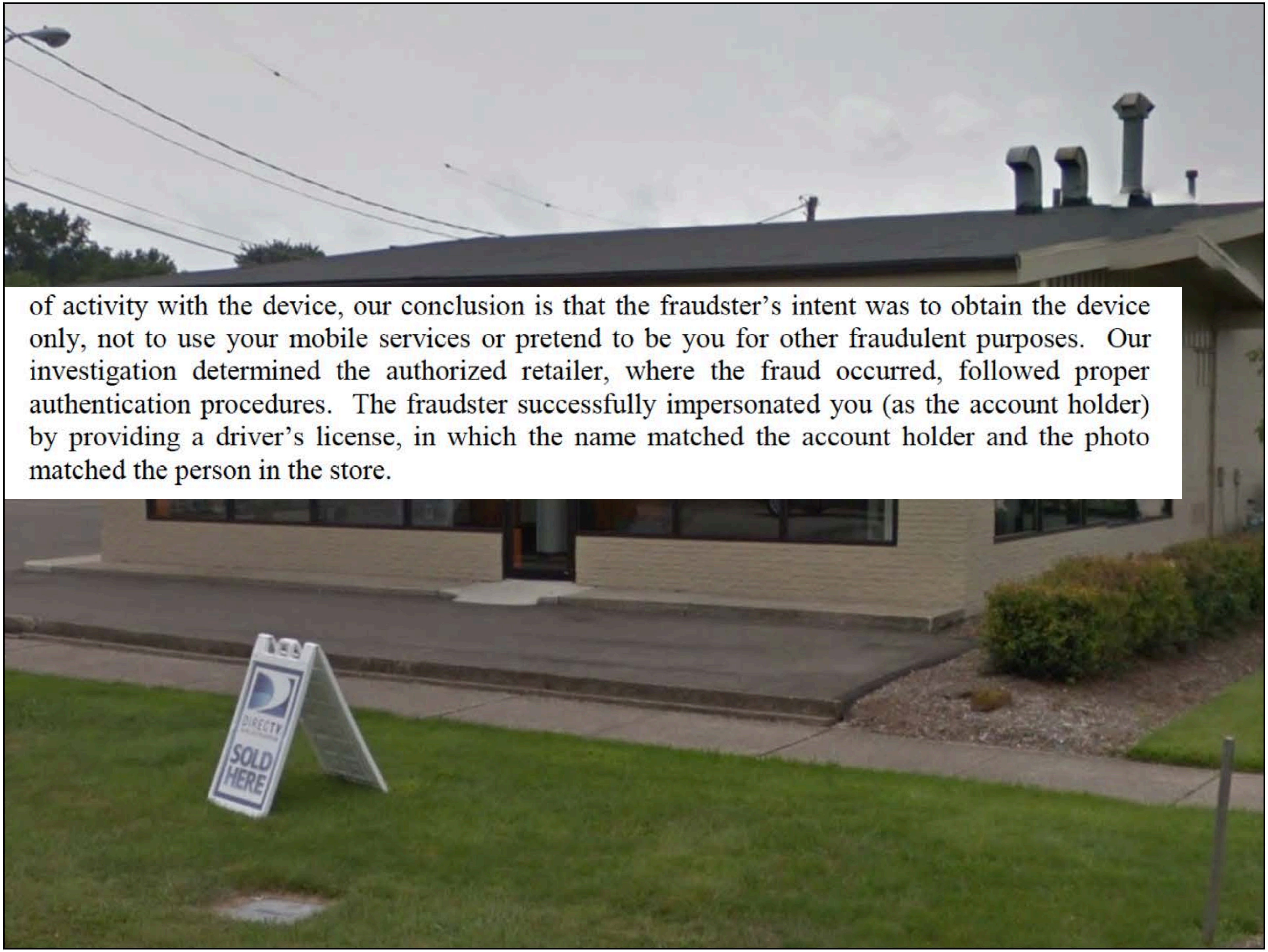
I am a victim of identity theft. The thief **[made a fraudulent transaction/opened a fraudulent account]** in my name with your company. In accordance with section 609(e) of the Fair Credit Reporting Act, 15 U.S.C. § 1681g(e), I am requesting that you provide me copies of business records relating to the fraudulent **[transaction/account]** identified above. The law directs that you provide these documents at no charge, and without requiring a subpoena, within thirty (30) days of your receipt of this request. I am enclosing a copy of the relevant federal law and the Federal Trade Commission's business



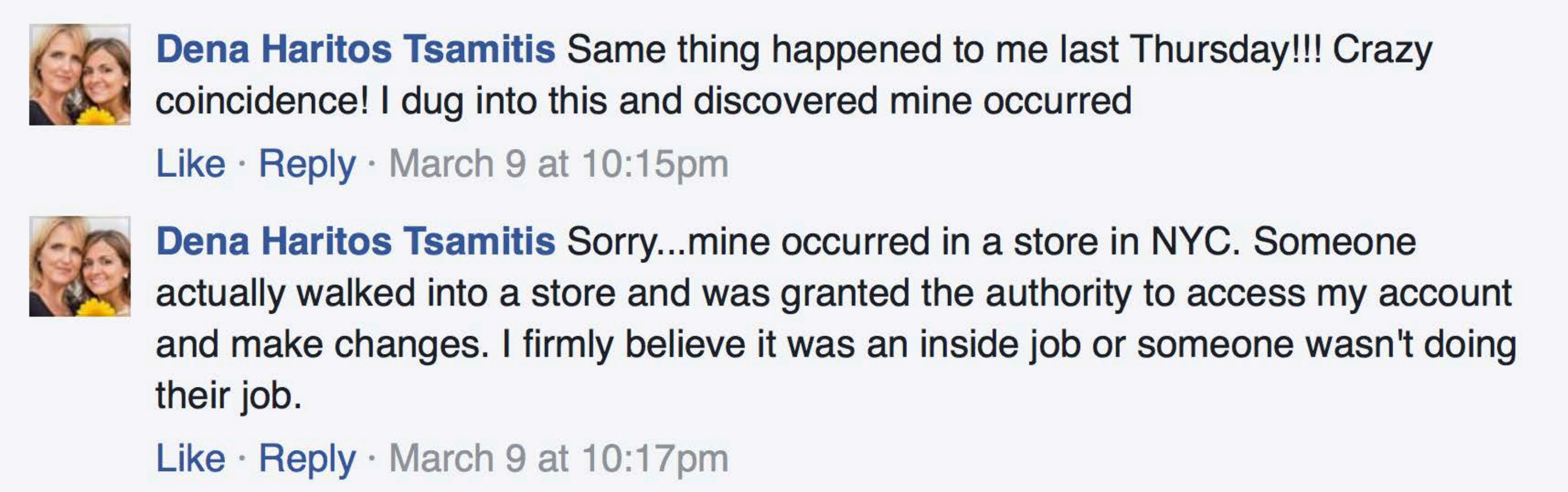
* 957 NSE 1 16C0203/24/16

RETURN TO SENDER
NOT DELIVERABLE AS ADDRESSED
UNABLE TO FORWARD

BC: 15217112932 *1443-04015-14-41



of activity with the device, our conclusion is that the fraudster's intent was to obtain the device only, not to use your mobile services or pretend to be you for other fraudulent purposes. Our investigation determined the authorized retailer, where the fraud occurred, followed proper authentication procedures. The fraudster successfully impersonated you (as the account holder) by providing a driver's license, in which the name matched the account holder and the photo matched the person in the store.

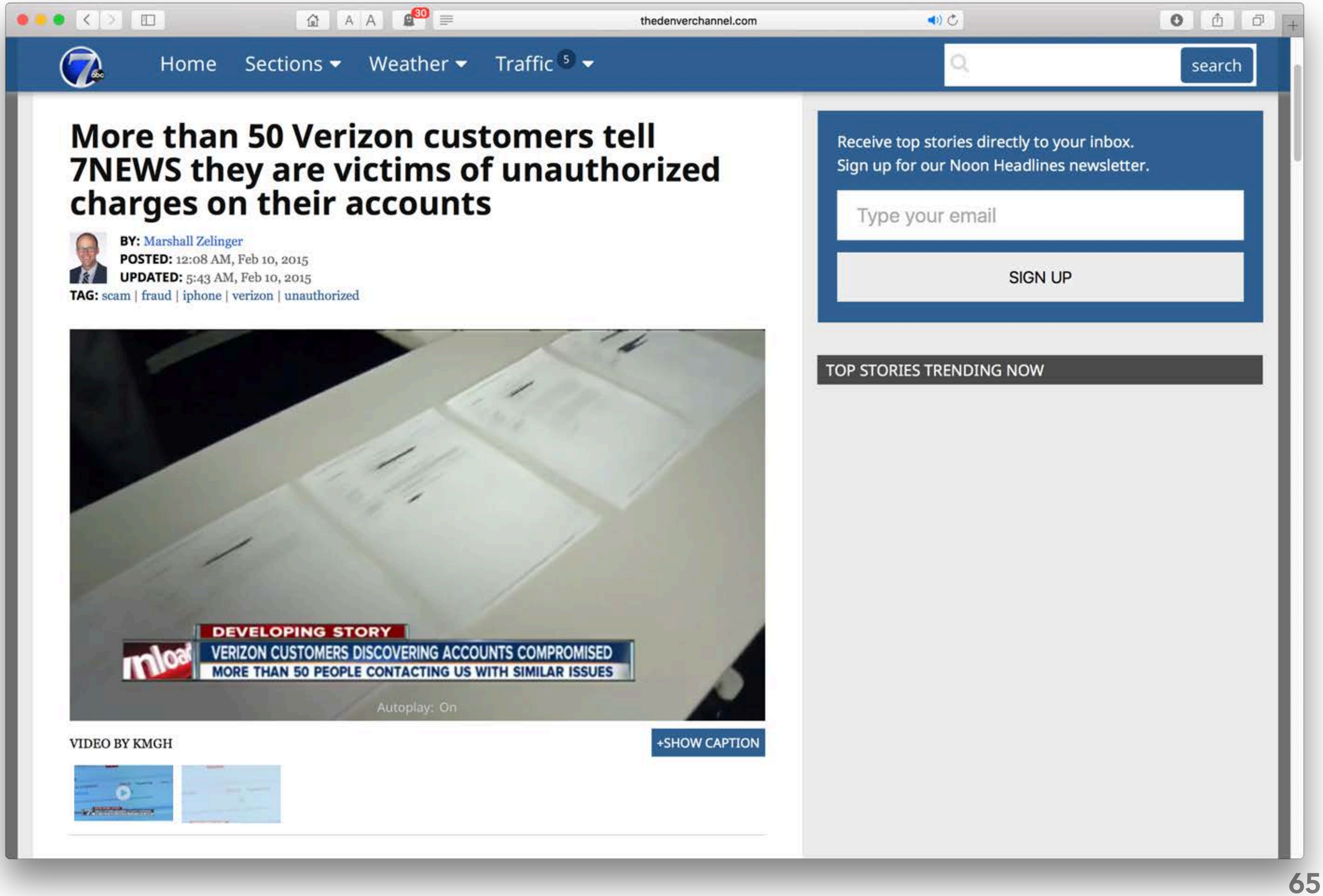


Dena Haritos Tsamitis Same thing happened to me last Thursday!!! Crazy coincidence! I dug into this and discovered mine occurred

Like · Reply · March 9 at 10:15pm

Dena Haritos Tsamitis Sorry...mine occurred in a store in NYC. Someone actually walked into a store and was granted the authority to access my account and make changes. I firmly believe it was an inside job or someone wasn't doing their job.

Like · Reply · March 9 at 10:17pm



More than 50 Verizon customers tell 7NEWS they are victims of unauthorized charges on their accounts

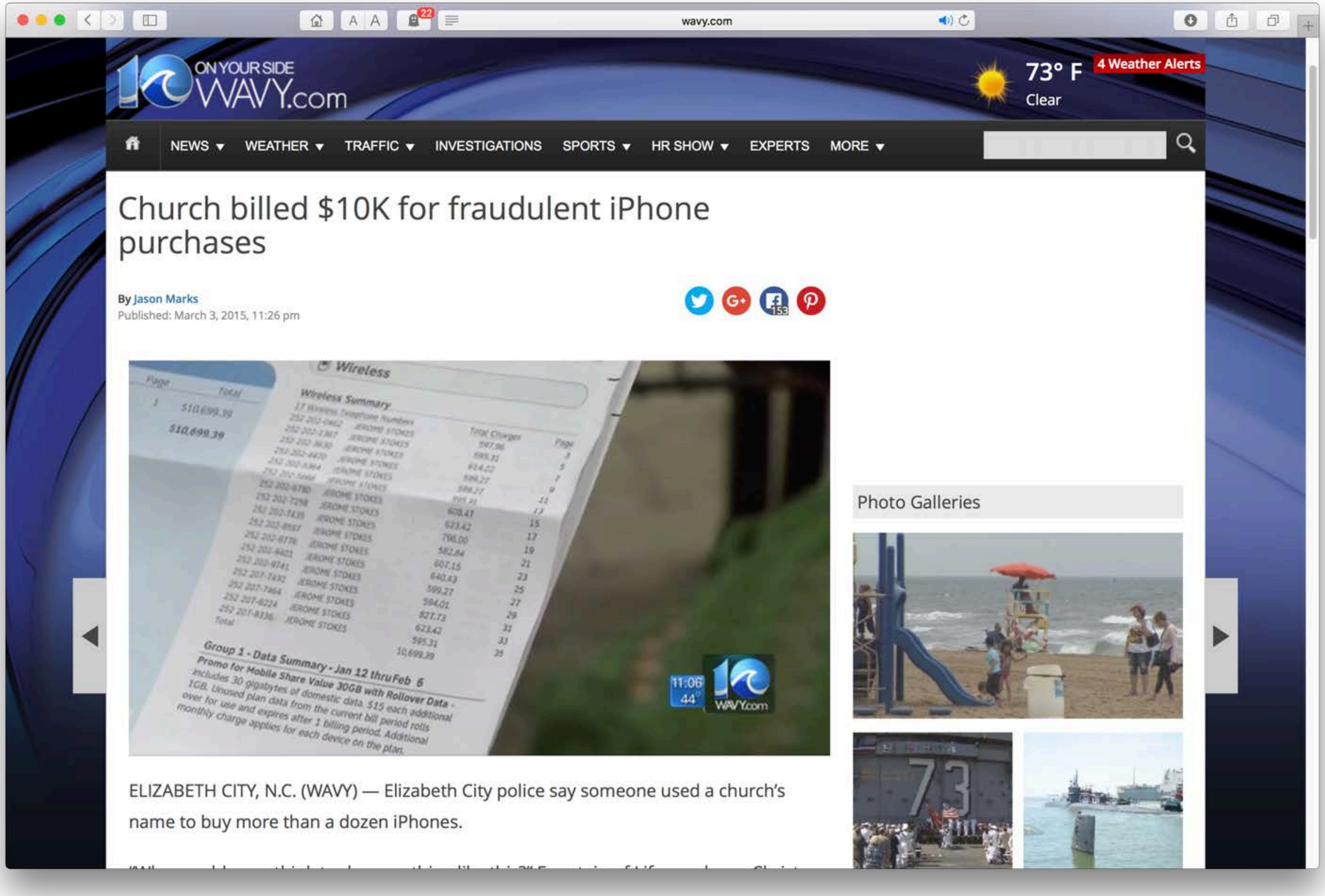
BY: Marshall Zelinger
POSTED: 12:08 AM, Feb 10, 2015
UPDATED: 5:43 AM, Feb 10, 2015
TAG: scam | fraud | iphone | verizon | unauthorized

VIDEO BY KMGH

Receive top stories directly to your inbox.
Sign up for our Noon Headlines newsletter.

Type your email

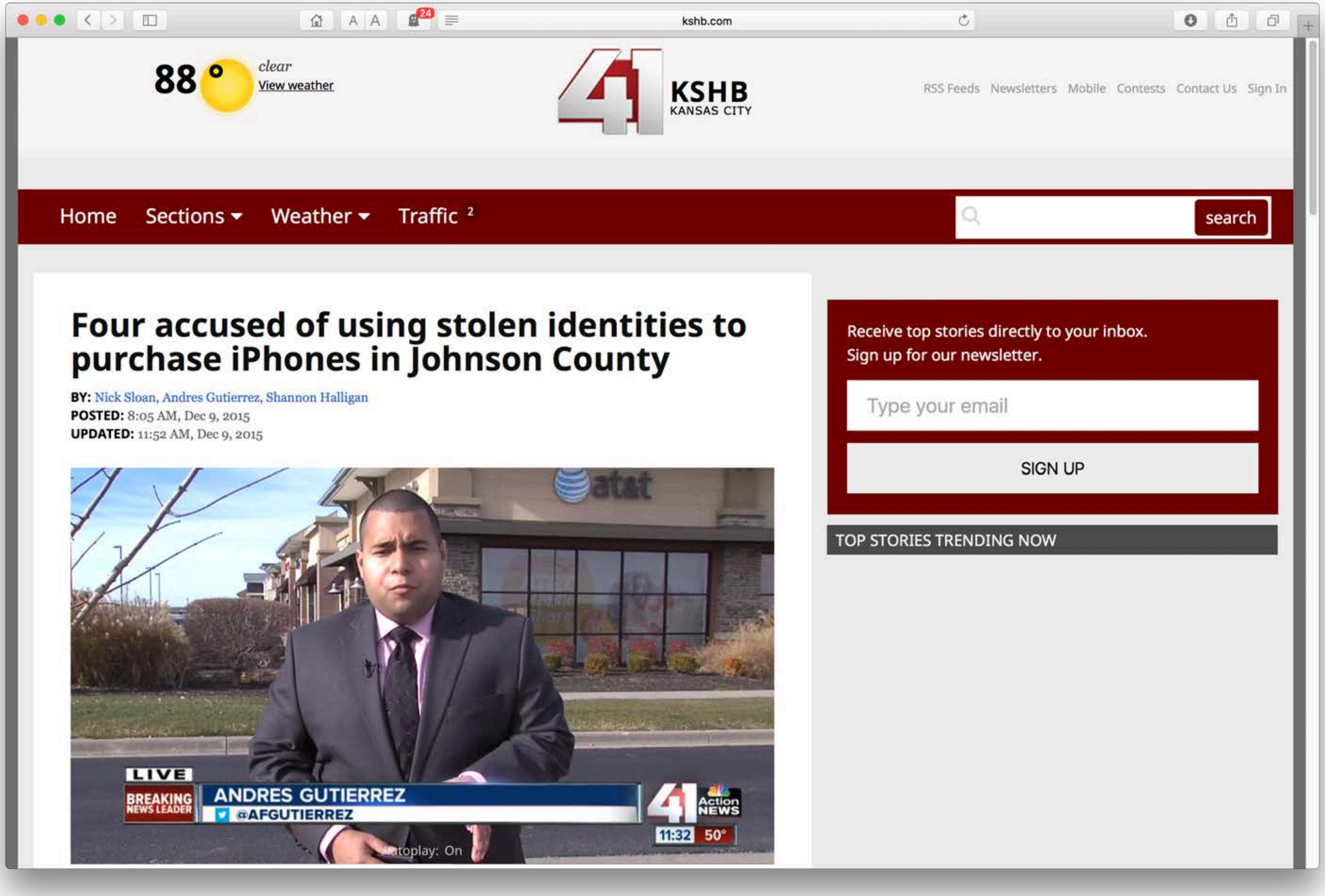
SIGN UP



Church billed $10K for fraudulent iPhone purchases

By Jason Marks
Published: March 3, 2015, 11:26 pm

ELIZABETH CITY, N.C. (WAVY) — Elizabeth City police say someone used a church's name to buy more than a dozen iPhones.



Four accused of using stolen identities to purchase iPhones in Johnson County

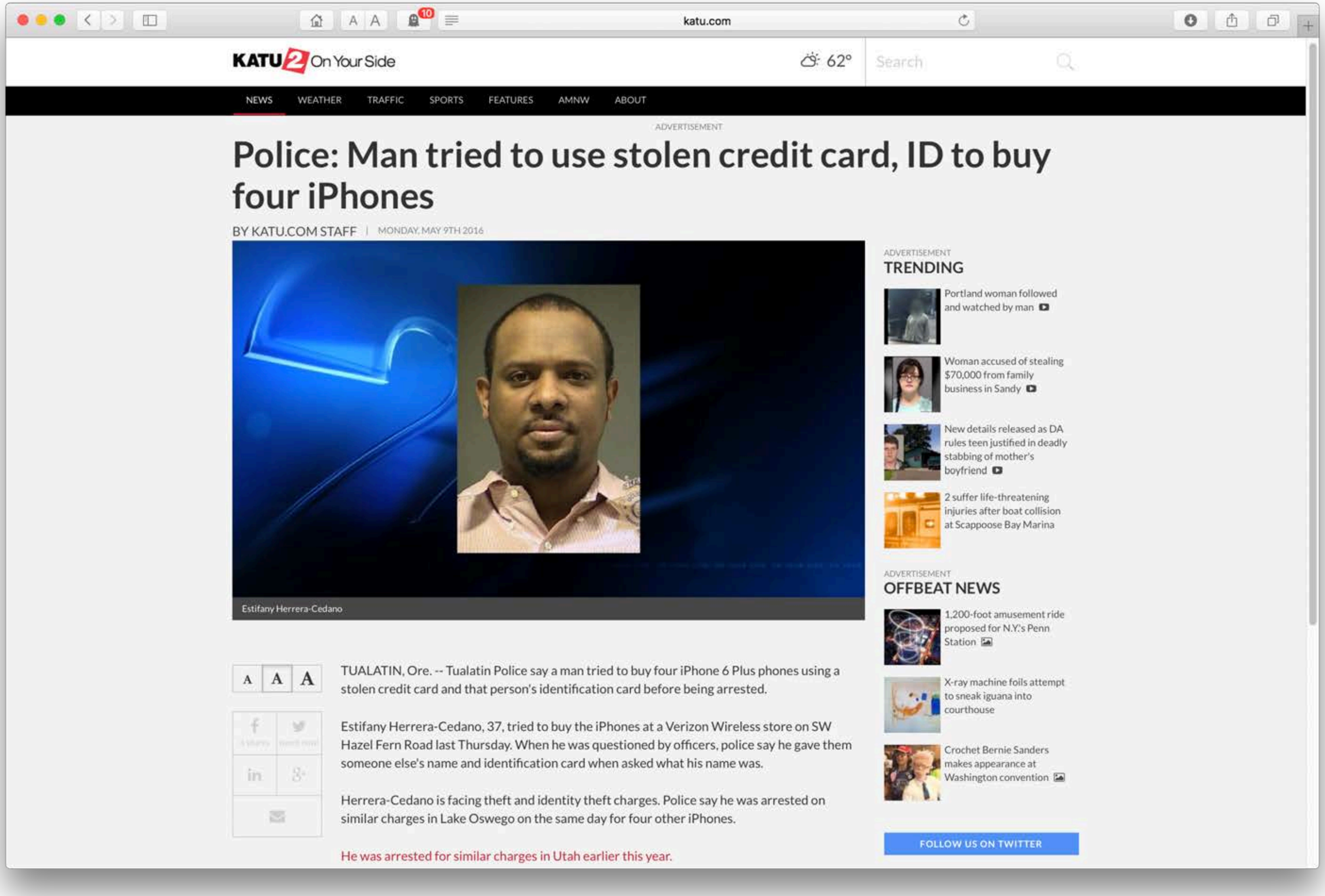
BY: Nick Sloan, Andres Gutierrez, Shannon Halligan
POSTED: 8:05 AM, Dec 9, 2015
UPDATED: 11:52 AM, Dec 9, 2015

Receive top stories directly to your inbox.
Sign up for our newsletter.

Type your email

SIGN UP

TOP STORIES TRENDING NOW



ADVERTISEMENT

Police: Man tried to use stolen credit card, ID to buy four iPhones

BY KATU.COM STAFF | MONDAY, MAY 9TH 2016

Estifany Herrera-Cedano

TUALATIN, Ore. -- Tualatin Police say a man tried to buy four iPhone 6 Plus phones using a stolen credit card and that person's identification card before being arrested.

Estifany Herrera-Cedano, 37, tried to buy the iPhones at a Verizon Wireless store on SW Hazel Fern Road last Thursday. When he was questioned by officers, police say he gave them someone else's name and identification card when asked what his name was.

Herrera-Cedano is facing theft and identity theft charges. Police say he was arrested on similar charges in Lake Oswego on the same day for four other iPhones.

He was arrested for similar charges in Utah earlier this year.

ADVERTISEMENT

TRENDING

Portland woman followed and watched by man

Woman accused of stealing $70,000 from family business in Sandy

New details released as DA rules teen justified in deadly stabbing of mother's boyfriend

2 suffer life-threatening injuries after boat collision at Scappoose Bay Marina

ADVERTISEMENT

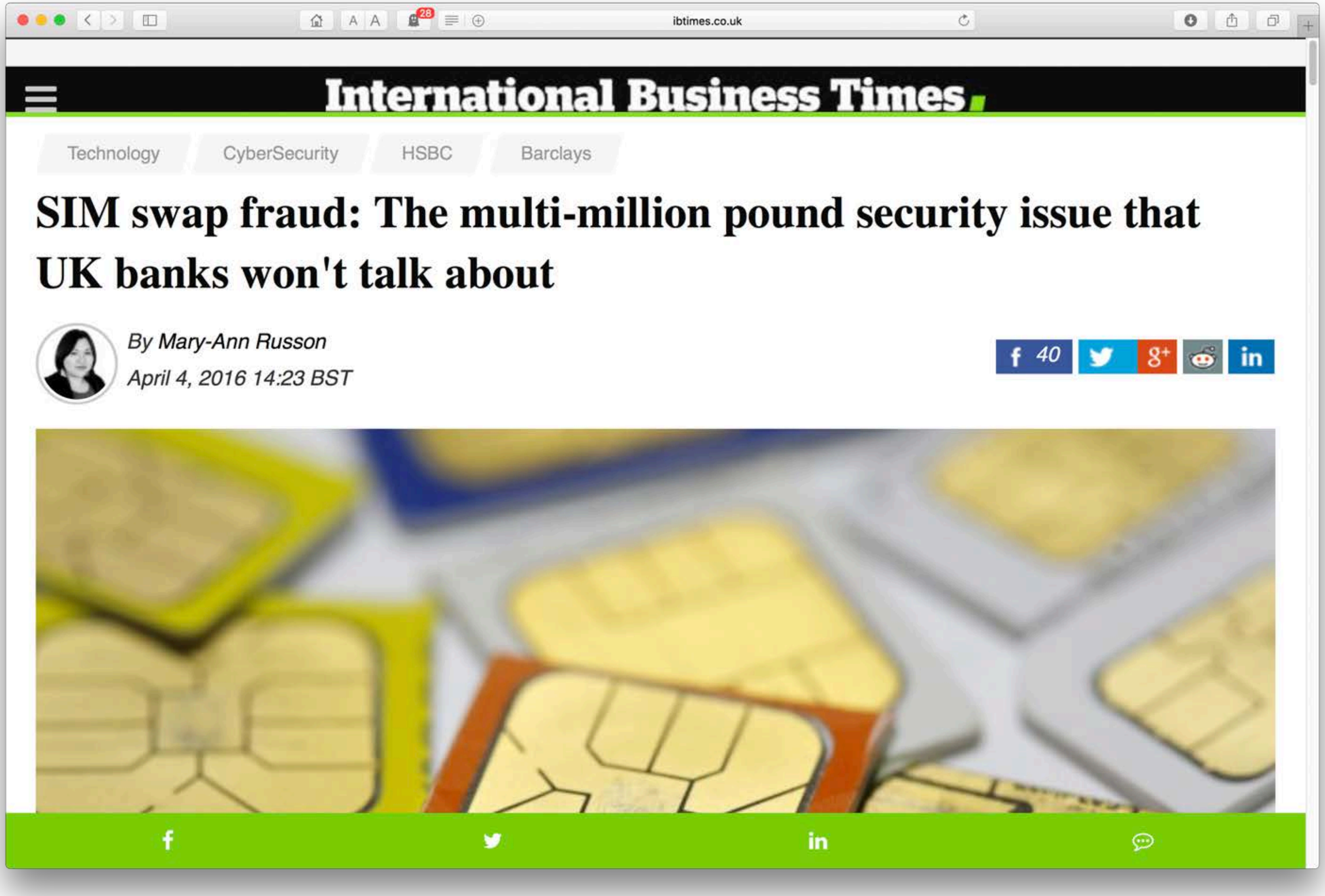
OFFBEAT NEWS

1,200-foot amusement ride proposed for N.Y.'s Penn Station

X-ray machine foils attempt to sneak iguana into courthouse

Crochet Bernie Sanders makes appearance at Washington convention

FOLLOW US ON TWITTER



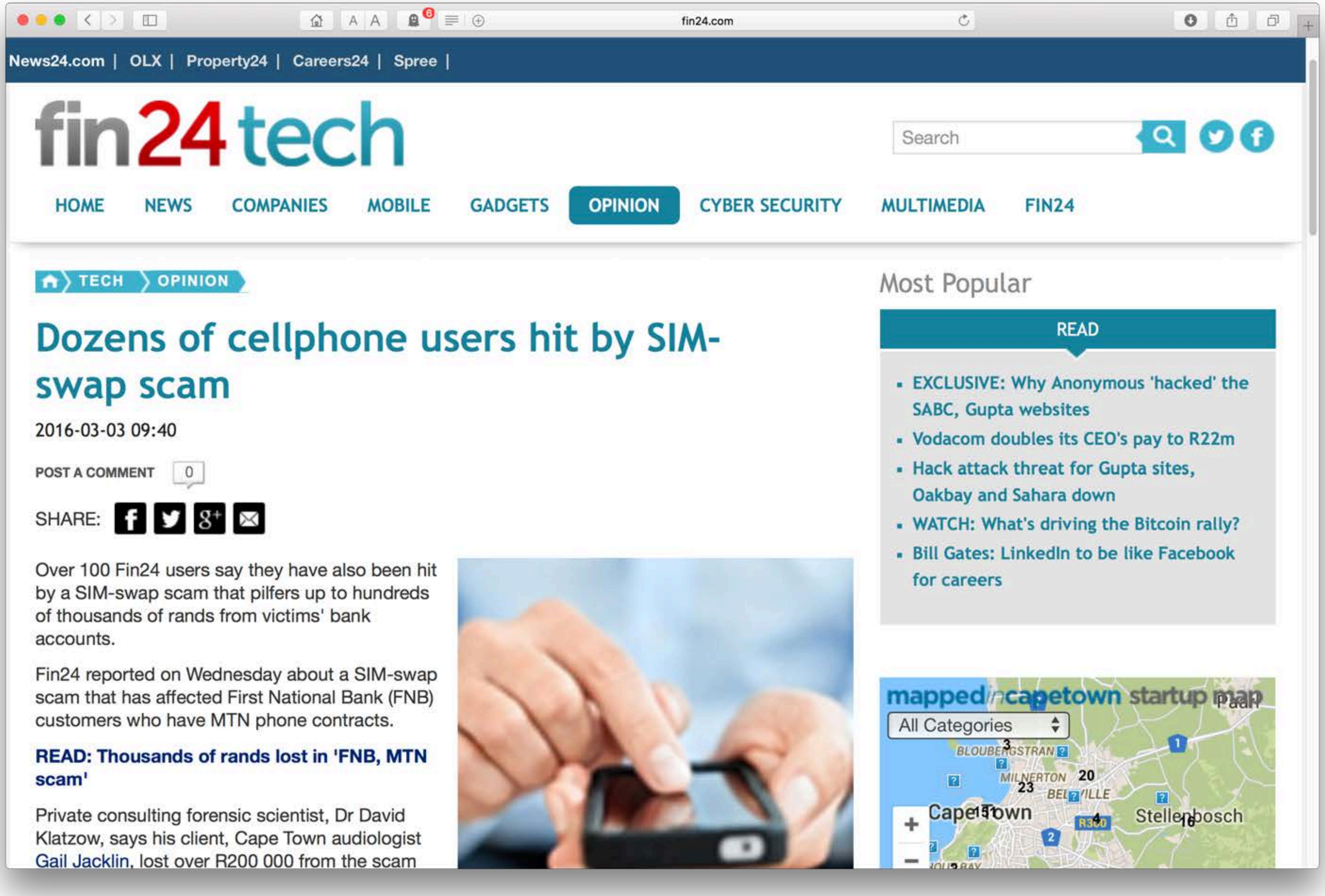
International Business Times

Technology CyberSecurity HSBC Barclays

SIM swap fraud: The multi-million pound security issue that UK banks won't talk about

By Mary-Ann Russon

April 4, 2016 14:23 BST



Dozens of cellphone users hit by SIM-swap scam

2016-03-03 09:40

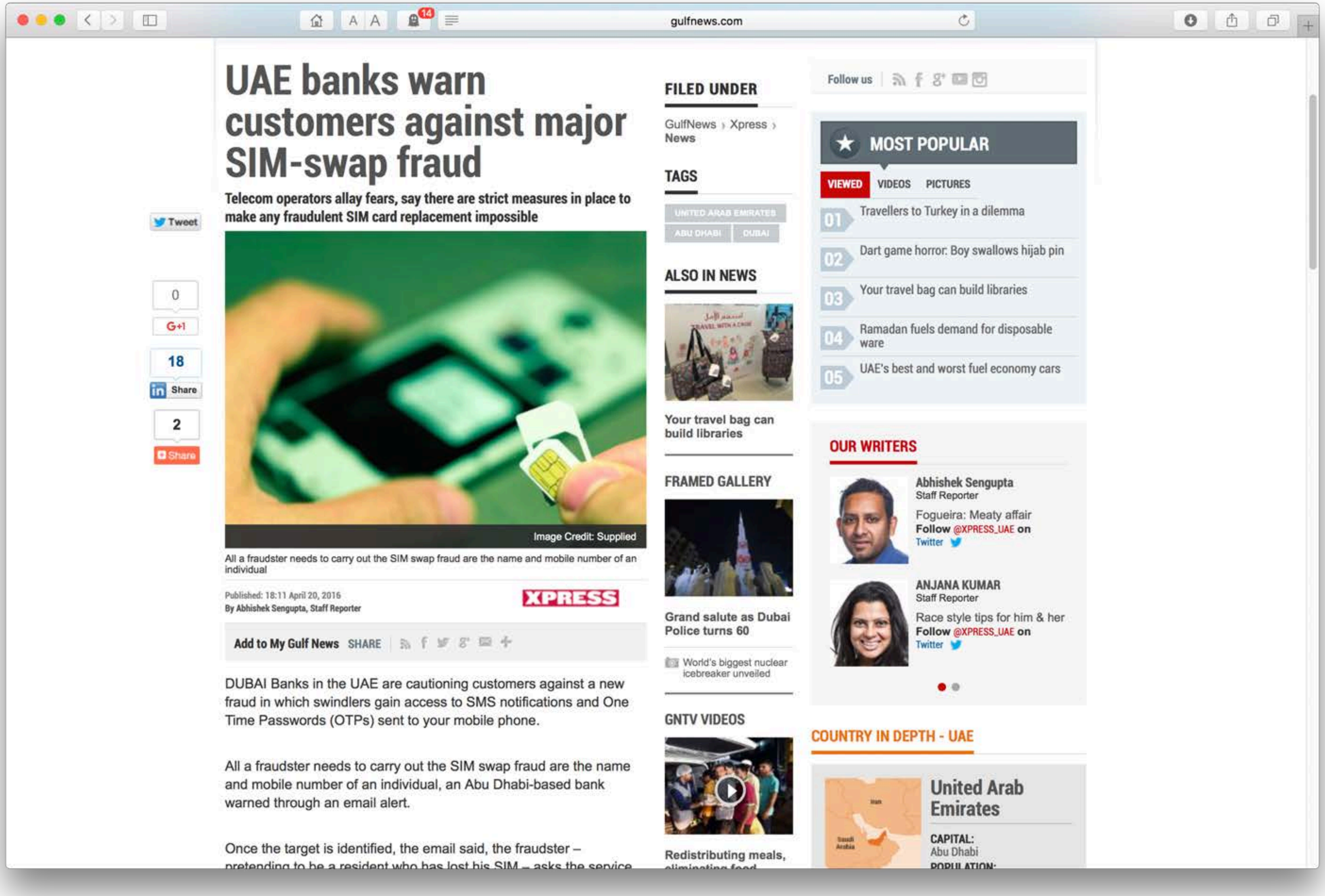
Over 100 Fin24 users say they have also been hit by a SIM-swap scam that pilfers up to hundreds of thousands of rands from victims' bank accounts.

Fin24 reported on Wednesday about a SIM-swap scam that has affected First National Bank (FNB) customers who have MTN phone contracts.

READ: Thousands of rands lost in 'FNB, MTN scam'

Private consulting forensic scientist, Dr David Klatzow, says his client, Cape Town audiologist Gail Jacklin, lost over R200 000 from the scam

- EXCLUSIVE: Why Anonymous 'hacked' the SABC, Gupta websites
- Vodacom doubles its CEO's pay to R22m
- Hack attack threat for Gupta sites, Oakbay and Sahara down
- WATCH: What's driving the Bitcoin rally?
- Bill Gates: LinkedIn to be like Facebook for careers



UAE banks warn customers against major SIM-swap fraud

Telecom operators allay fears, say there are strict measures in place to make any fraudulent SIM card replacement impossible

Image Credit: Supplied

All a fraudster needs to carry out the SIM swap fraud are the name and mobile number of an individual

Published: 18:11 April 20, 2016
By Abhishek Sengupta, Staff Reporter

XPRESS

Add to My Gulf News SHARE

DUBAI Banks in the UAE are cautioning customers against a new fraud in which swindlers gain access to SMS notifications and One Time Passwords (OTPs) sent to your mobile phone.

All a fraudster needs to carry out the SIM swap fraud are the name and mobile number of an individual, an Abu Dhabi-based bank warned through an email alert.

Once the target is identified, the email said, the fraudster – pretending to be a resident who has lost his SIM – asks the service

FILED UNDER

GulfNews › Xpress › News

TAGS

UNITED ARAB EMIRATES
ABU DHABI
DUBAI

ALSO IN NEWS

Your travel bag can build libraries

FRAMED GALLERY

Grand salute as Dubai Police turns 60

World's biggest nuclear icebreaker unveiled

GNTV VIDEOS

Redistributing meals, eliminating food

Follow us

MOST POPULAR

VIEWED VIDEOS PICTURES

01 Travellers to Turkey in a dilemma
02 Dart game horror: Boy swallows hijab pin
03 Your travel bag can build libraries
04 Ramadan fuels demand for disposable ware
05 UAE's best and worst fuel economy cars

OUR WRITERS

Abhishek Sengupta
Staff Reporter
Fogueira: Meaty affair
Follow @XPRESS_UAE **on** Twitter

ANJANA KUMAR
Staff Reporter
Race style tips for him & her
Follow @XPRESS_UAE **on** Twitter

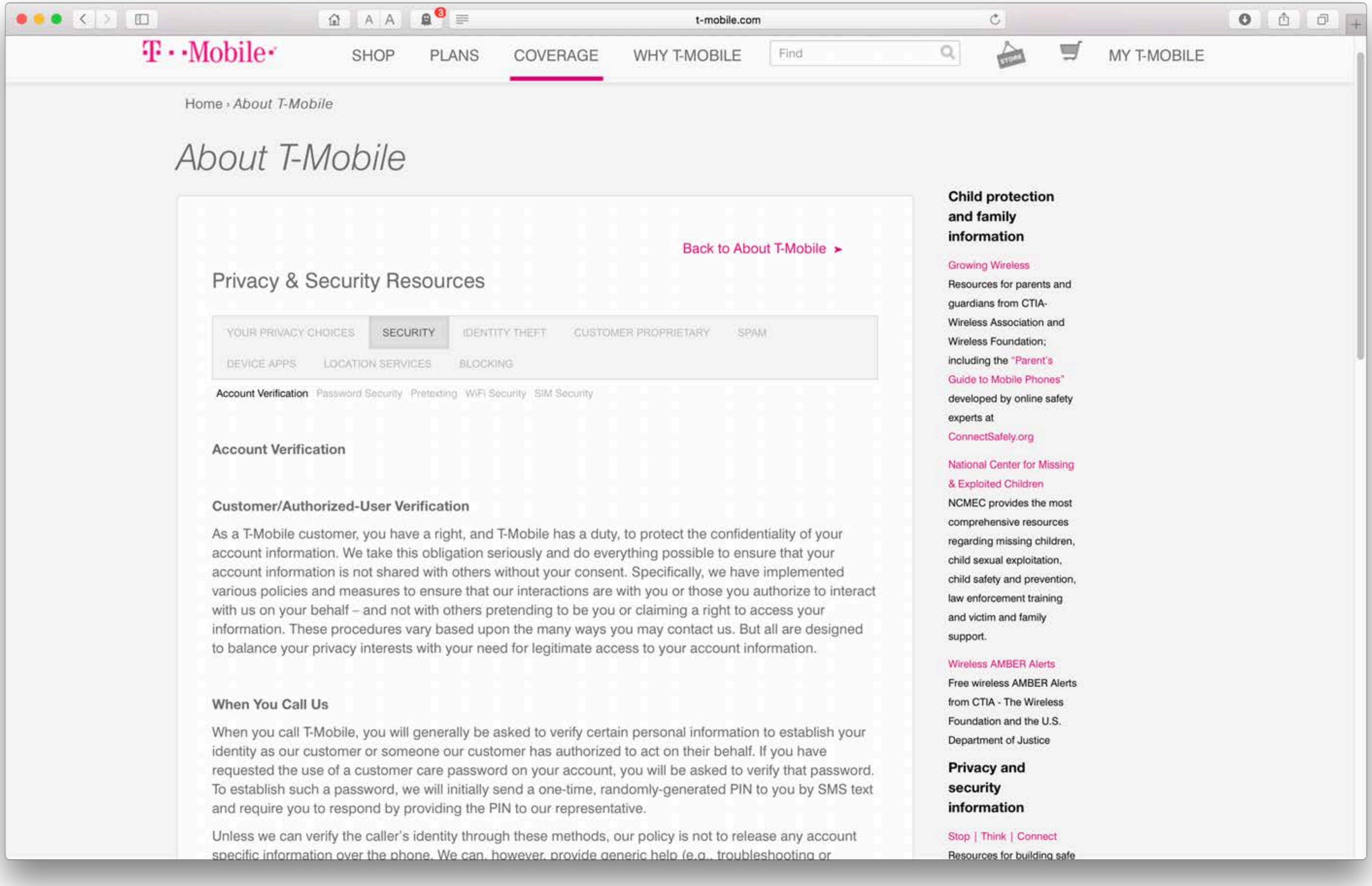
COUNTRY IN DEPTH - UAE

United Arab Emirates

CAPITAL:
Abu Dhabi
POPULATION:

Mobile phone account hijacking and new account fraud

	Number of incidents reported	% of identity theft reports
January 2013	1,083	3.2%
January 2016	2,658	6.3%



Home › *About T-Mobile*

About T-Mobile

Back to About T-Mobile ➤

Privacy & Security Resources

Account Verification

Customer/Authorized-User Verification

As a T-Mobile customer, you have a right, and T-Mobile has a duty, to protect the confidentiality of your account information. We take this obligation seriously and do everything possible to ensure that your account information is not shared with others without your consent. Specifically, we have implemented various policies and measures to ensure that our interactions are with you or those you authorize to interact with us on your behalf – and not with others pretending to be you or claiming a right to access your information. These procedures vary based upon the many ways you may contact us. But all are designed to balance your privacy interests with your need for legitimate access to your account information.

When You Call Us

When you call T-Mobile, you will generally be asked to verify certain personal information to establish your identity as our customer or someone our customer has authorized to act on their behalf. If you have requested the use of a customer care password on your account, you will be asked to verify that password. To establish such a password, we will initially send a one-time, randomly-generated PIN to you by SMS text and require you to respond by providing the PIN to our representative.

Unless we can verify the caller's identity through these methods, our policy is not to release any account specific information over the phone. We can, however, provide generic help (e.g., troubleshooting or

Child protection and family information

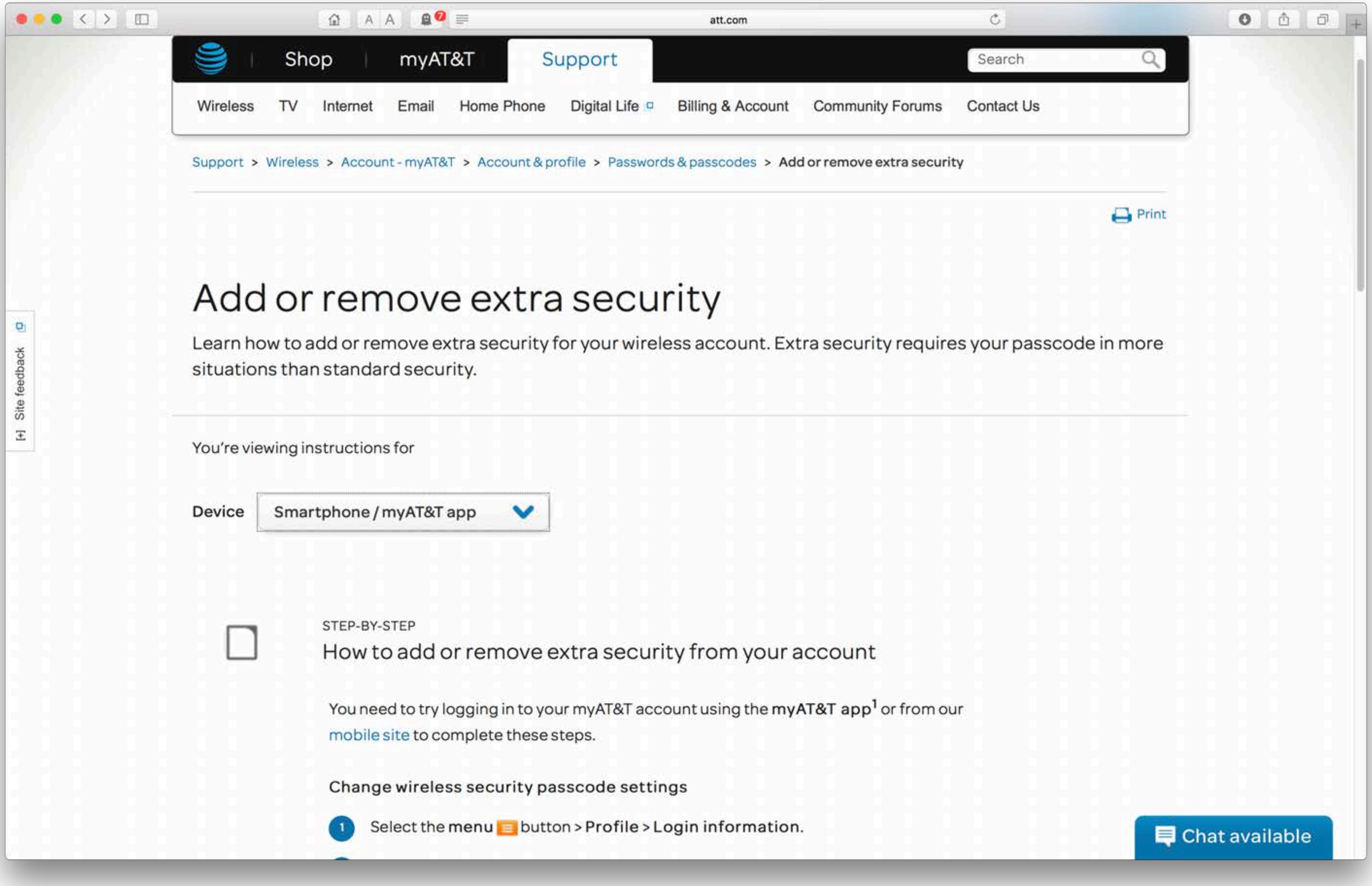
Growing Wireless
Resources for parents and guardians from CTIA-Wireless Association and Wireless Foundation; including the "Parent's Guide to Mobile Phones" developed by online safety experts at ConnectSafely.org

National Center for Missing & Exploited Children
NCMEC provides the most comprehensive resources regarding missing children, child sexual exploitation, child safety and prevention, law enforcement training and victim and family support.

Wireless AMBER Alerts
Free wireless AMBER Alerts from CTIA - The Wireless Foundation and the U.S. Department of Justice

Privacy and security information

Stop | Think | Connect
Resources for building safe



Add or remove extra security

Learn how to add or remove extra security for your wireless account. Extra security requires your passcode in more situations than standard security.

You're viewing instructions for

Device Smartphone / myAT&T app

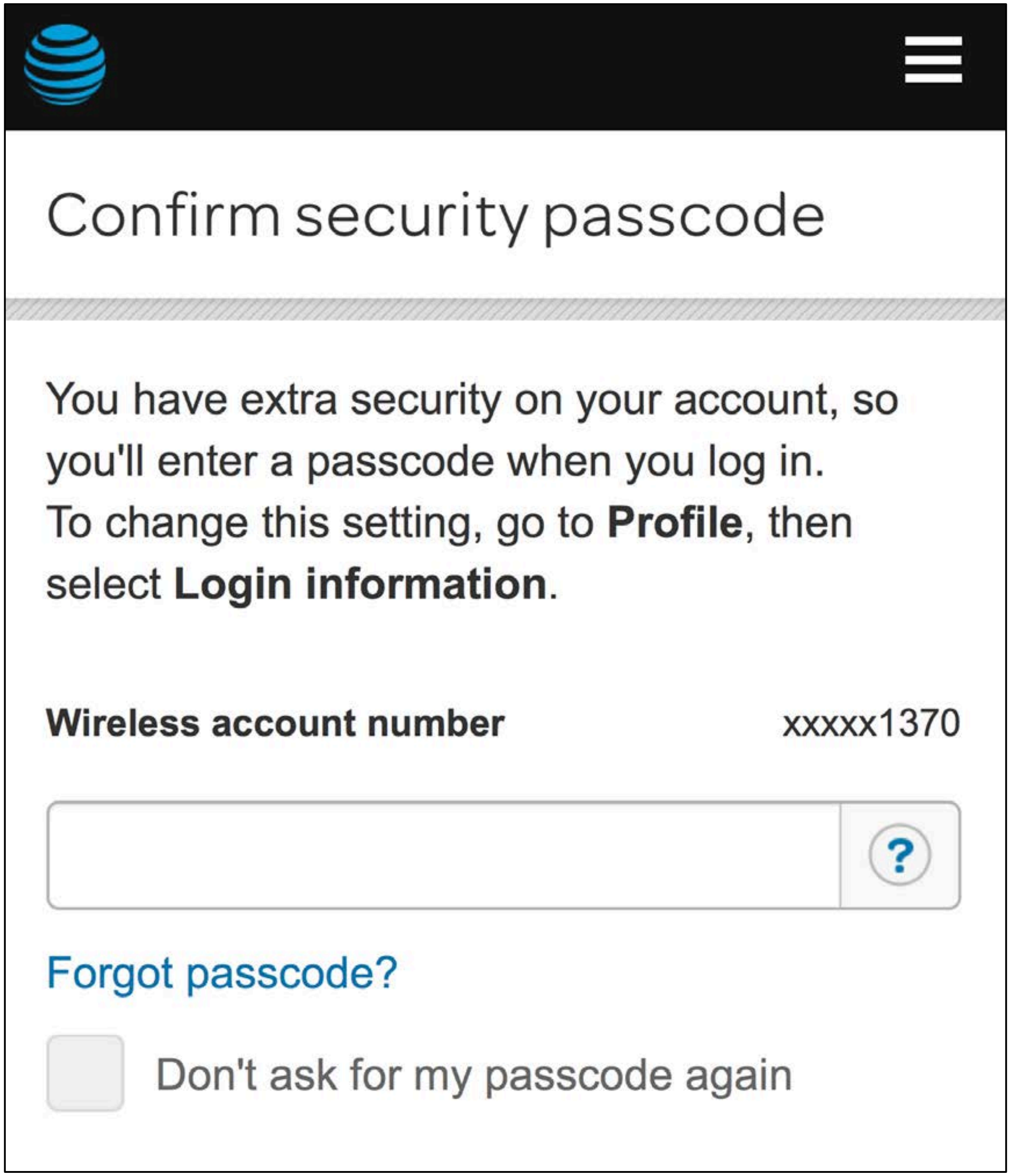
STEP-BY-STEP

How to add or remove extra security from your account

You need to try logging in to your myAT&T account using the **myAT&T app**[1] or from our mobile site to complete these steps.

Change wireless security passcode settings

1. Select the **menu** button > **Profile** > **Login information.**



Confirm security passcode

You have extra security on your account, so you'll enter a passcode when you log in. To change this setting, go to **Profile**, then select **Login information**.

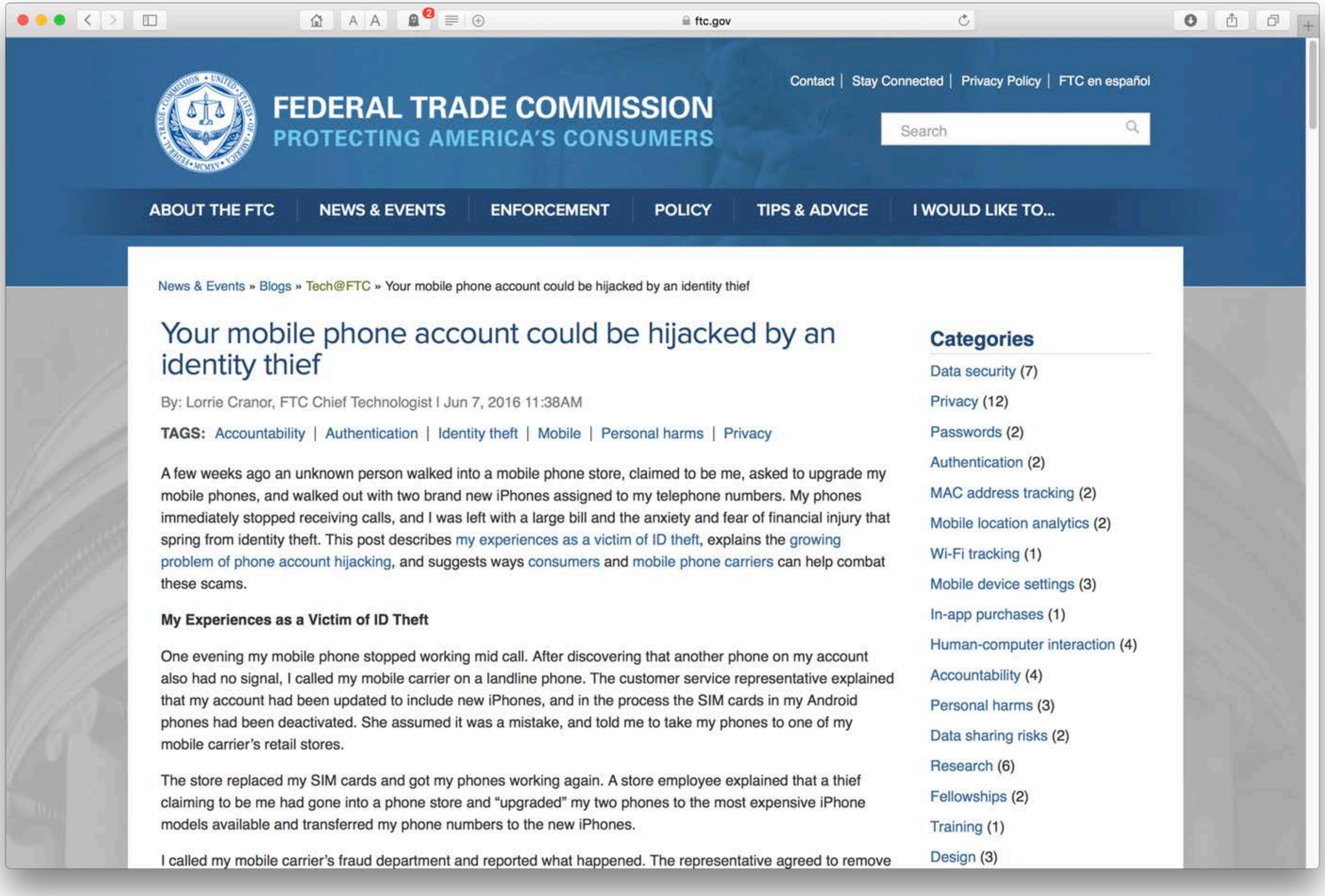
Wireless account number xxxxx1370

Forgot passcode?

□ Don't ask for my passcode again

verizon wireless

Sprint



News & Events » Blogs » Tech@FTC » Your mobile phone account could be hijacked by an identity thief

Your mobile phone account could be hijacked by an identity thief

By: Lorrie Cranor, FTC Chief Technologist l Jun 7, 2016 11:38AM

TAGS: Accountability | Authentication | Identity theft | Mobile | Personal harms | Privacy

A few weeks ago an unknown person walked into a mobile phone store, claimed to be me, asked to upgrade my mobile phones, and walked out with two brand new iPhones assigned to my telephone numbers. My phones immediately stopped receiving calls, and I was left with a large bill and the anxiety and fear of financial injury that spring from identity theft. This post describes my experiences as a victim of ID theft, explains the growing problem of phone account hijacking, and suggests ways consumers and mobile phone carriers can help combat these scams.

My Experiences as a Victim of ID Theft

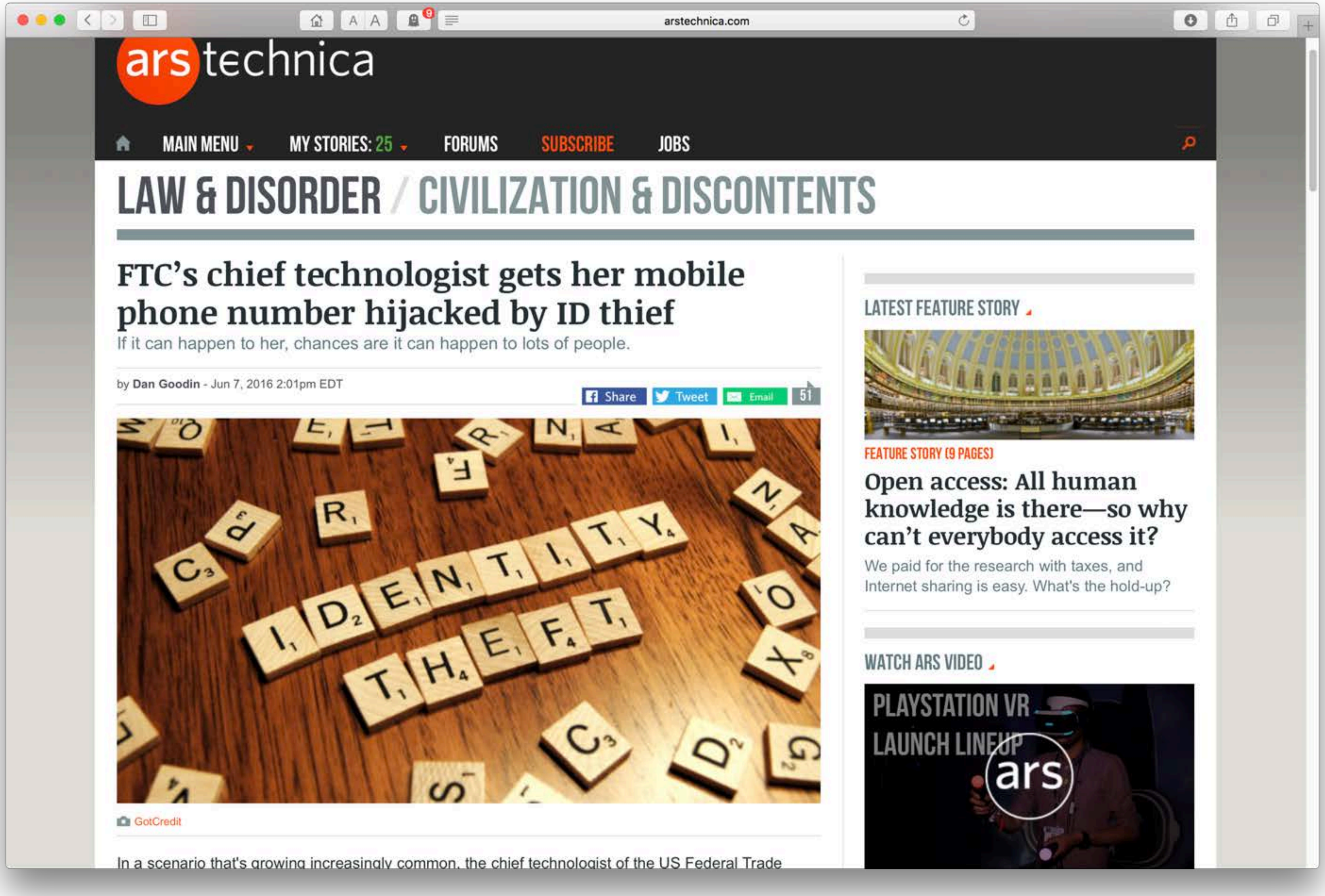
One evening my mobile phone stopped working mid call. After discovering that another phone on my account also had no signal, I called my mobile carrier on a landline phone. The customer service representative explained that my account had been updated to include new iPhones, and in the process the SIM cards in my Android phones had been deactivated. She assumed it was a mistake, and told me to take my phones to one of my mobile carrier's retail stores.

The store replaced my SIM cards and got my phones working again. A store employee explained that a thief claiming to be me had gone into a phone store and "upgraded" my two phones to the most expensive iPhone models available and transferred my phone numbers to the new iPhones.

I called my mobile carrier's fraud department and reported what happened. The representative agreed to remove

Categories

- Data security (7)
- Privacy (12)
- Passwords (2)
- Authentication (2)
- MAC address tracking (2)
- Mobile location analytics (2)
- Wi-Fi tracking (1)
- Mobile device settings (3)
- In-app purchases (1)
- Human-computer interaction (4)
- Accountability (4)
- Personal harms (3)
- Data sharing risks (2)
- Research (6)
- Fellowships (2)
- Training (1)
- Design (3)



LAW & DISORDER / CIVILIZATION & DISCONTENTS

FTC's chief technologist gets her mobile phone number hijacked by ID thief

If it can happen to her, chances are it can happen to lots of people.

by Dan Goodin - Jun 7, 2016 2:01pm EDT

In a scenario that's growing increasingly common, the chief technologist of the US Federal Trade

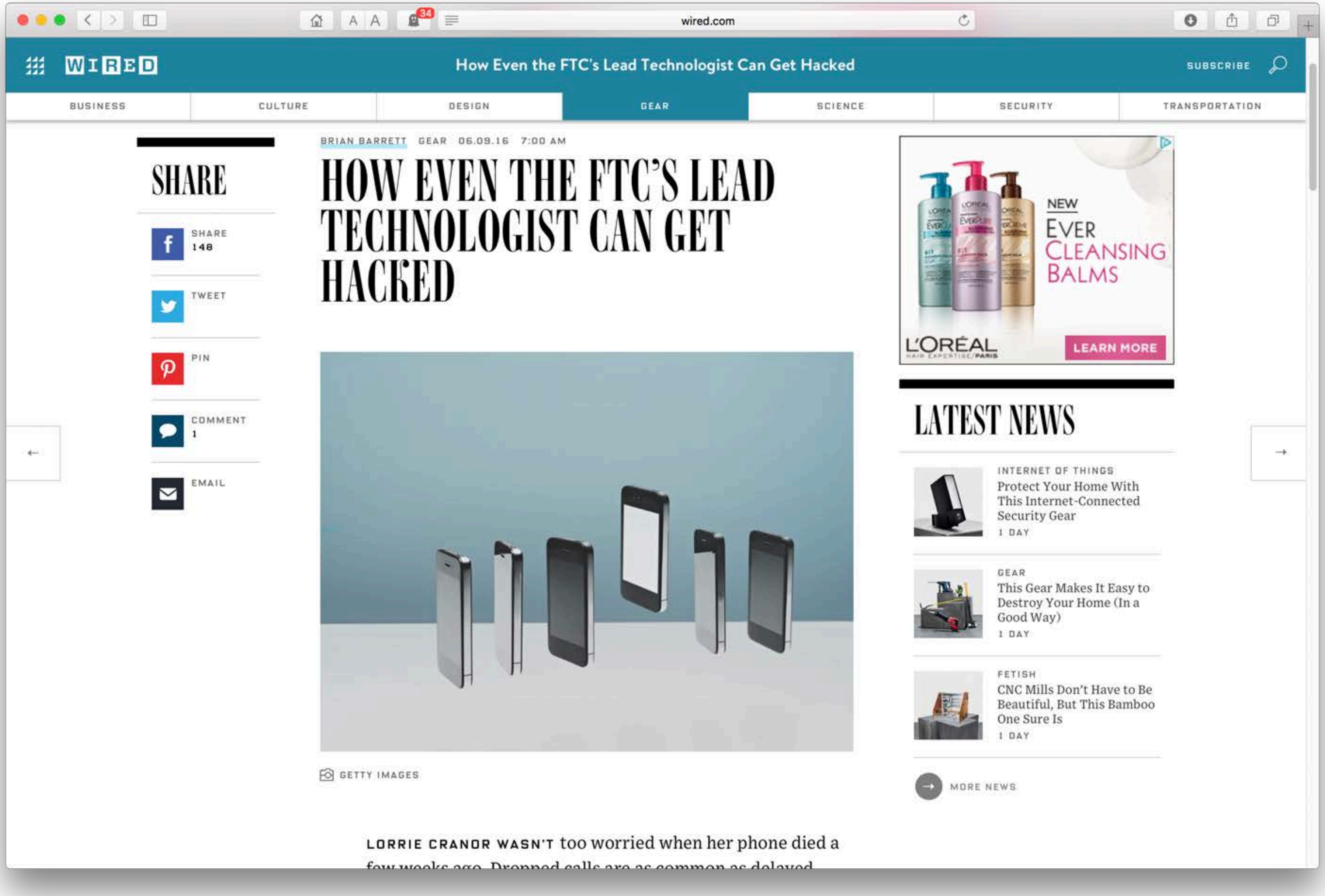
LATEST FEATURE STORY

FEATURE STORY (9 PAGES)

Open access: All human knowledge is there—so why can't everybody access it?

We paid for the research with taxes, and Internet sharing is easy. What's the hold-up?

WATCH ARS VIDEO



How Even the FTC's Lead Technologist Can Get Hacked

SHARE

BRIAN BARRETT GEAR 06.09.16 7:00 AM

HOW EVEN THE FTC'S LEAD TECHNOLOGIST CAN GET HACKED

GETTY IMAGES

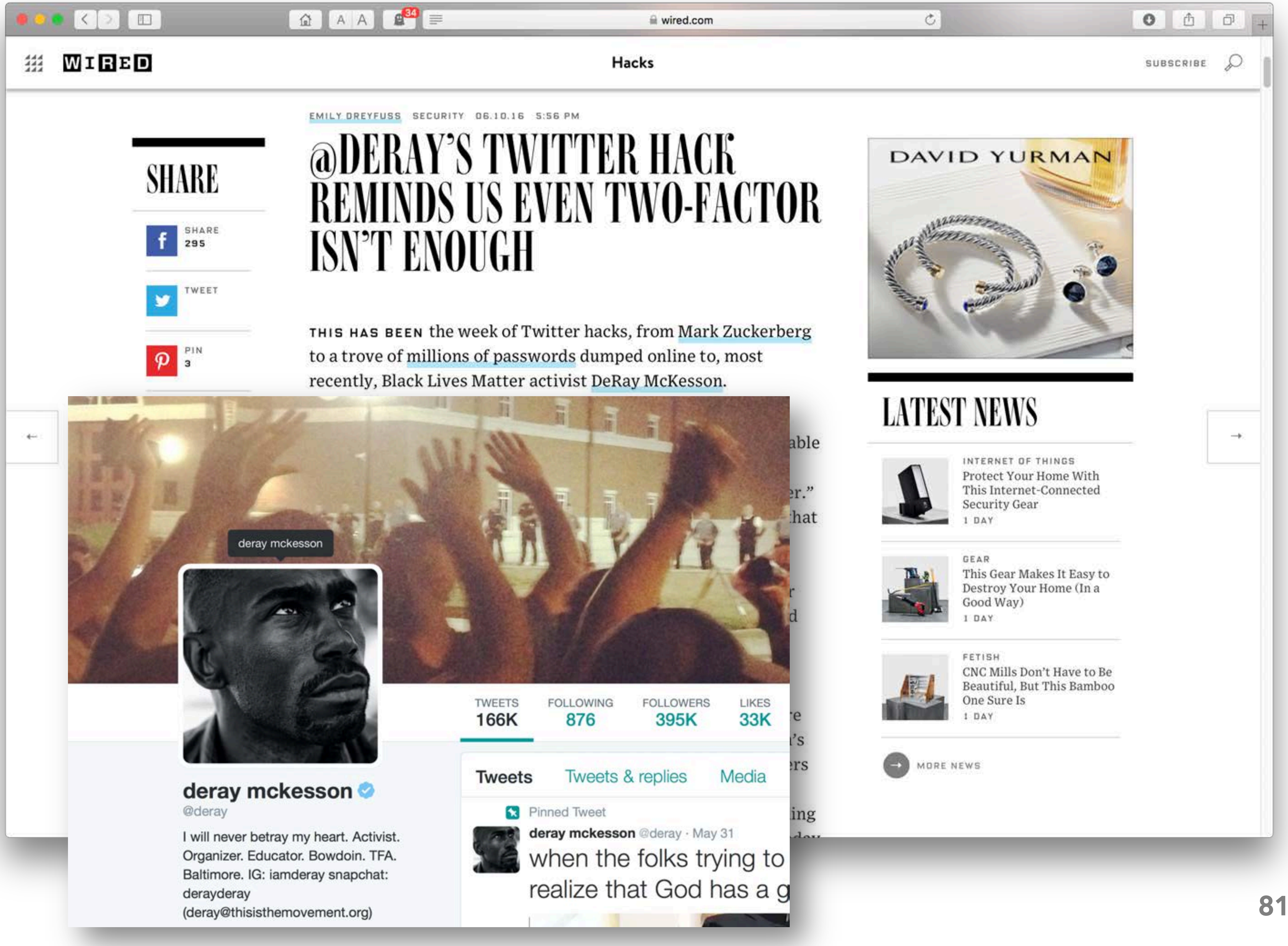
LORRIE CRANOR WASN'T too worried when her phone died a few weeks ago. Dropped calls are as common as delayed

LATEST NEWS

INTERNET OF THINGS
Protect Your Home With This Internet-Connected Security Gear
1 DAY

GEAR
This Gear Makes It Easy to Destroy Your Home (In a Good Way)
1 DAY

FETISH
CNC Mills Don't Have to Be Beautiful, But This Bamboo One Sure Is
1 DAY



EMILY DREYFUSS SECURITY 06.10.16 5:56 PM

@DERAY'S TWITTER HACK REMINDS US EVEN TWO-FACTOR ISN'T ENOUGH

THIS HAS BEEN the week of Twitter hacks, from Mark Zuckerberg to a trove of millions of passwords dumped online to, most recently, Black Lives Matter activist DeRay McKesson.

able
er.”
hat
r
d
e
's
ers
ing

LATEST NEWS

INTERNET OF THINGS
Protect Your Home With This Internet-Connected Security Gear
1 DAY

GEAR
This Gear Makes It Easy to Destroy Your Home (In a Good Way)
1 DAY

FETISH
CNC Mills Don't Have to Be Beautiful, But This Bamboo One Sure Is
1 DAY

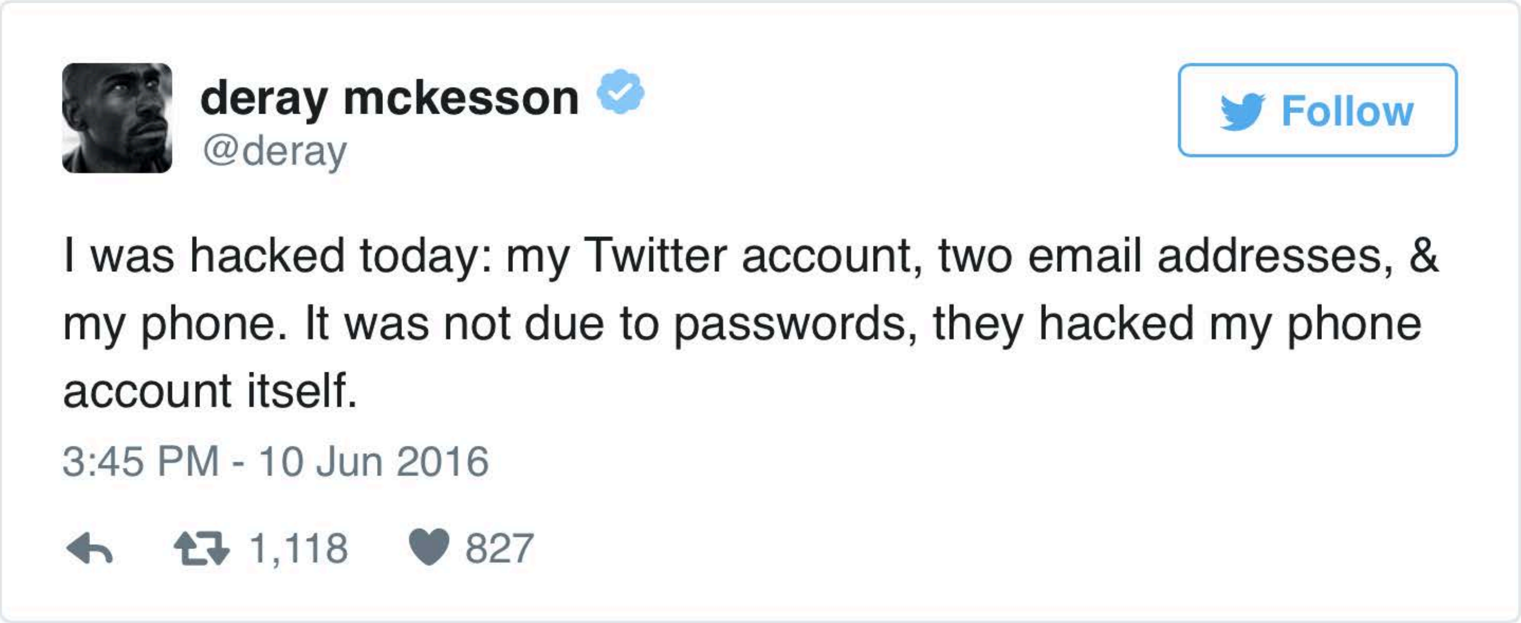
MORE NEWS

TWEETS	FOLLOWING	FOLLOWERS	LIKES
166K	876	395K	33K

deray mckesson
@deray

I will never betray my heart. Activist. Organizer. Educator. Bowdoin. TFA. Baltimore. IG: iamderay snapchat: deraydery (deray@thisisthemovement.org)

Pinned Tweet
deray mckesson @deray · May 31
when the folks trying to realize that God has a g

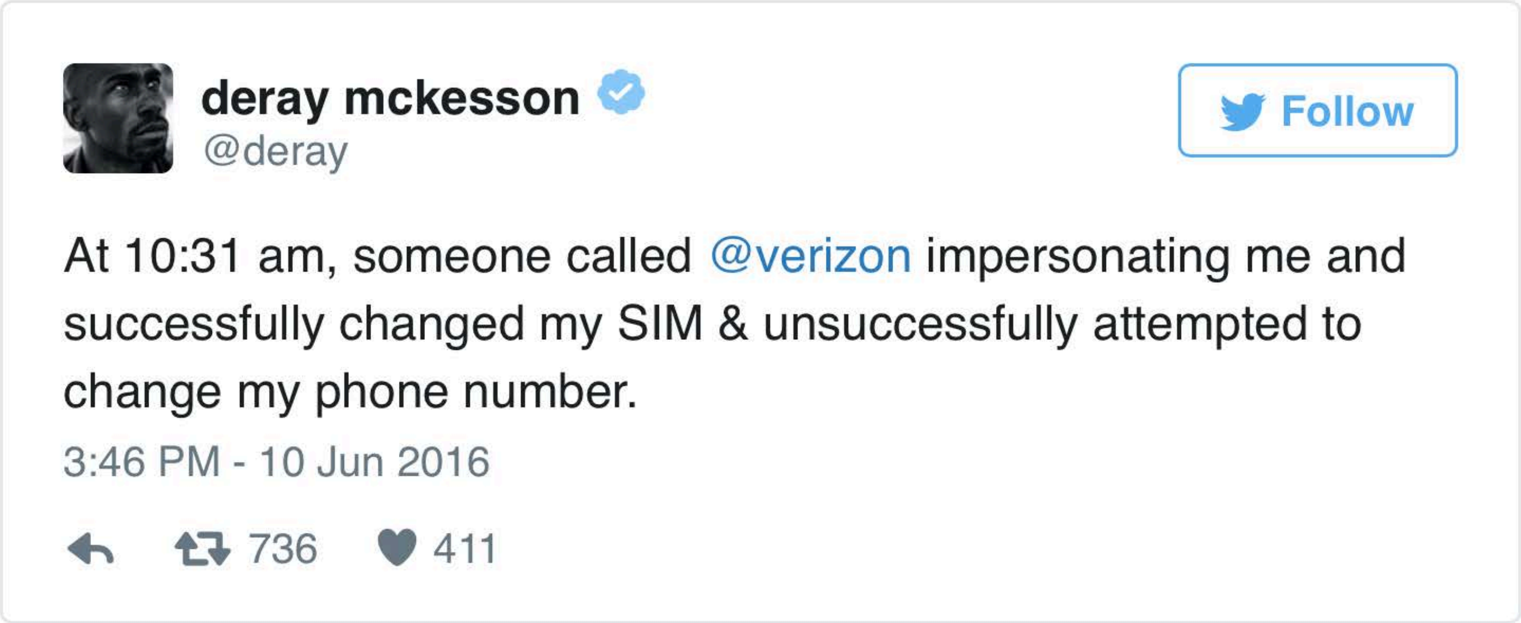


deray mckesson
@deray

I was hacked today: my Twitter account, two email addresses, & my phone. It was not due to passwords, they hacked my phone account itself.

3:45 PM - 10 Jun 2016

1,118 827

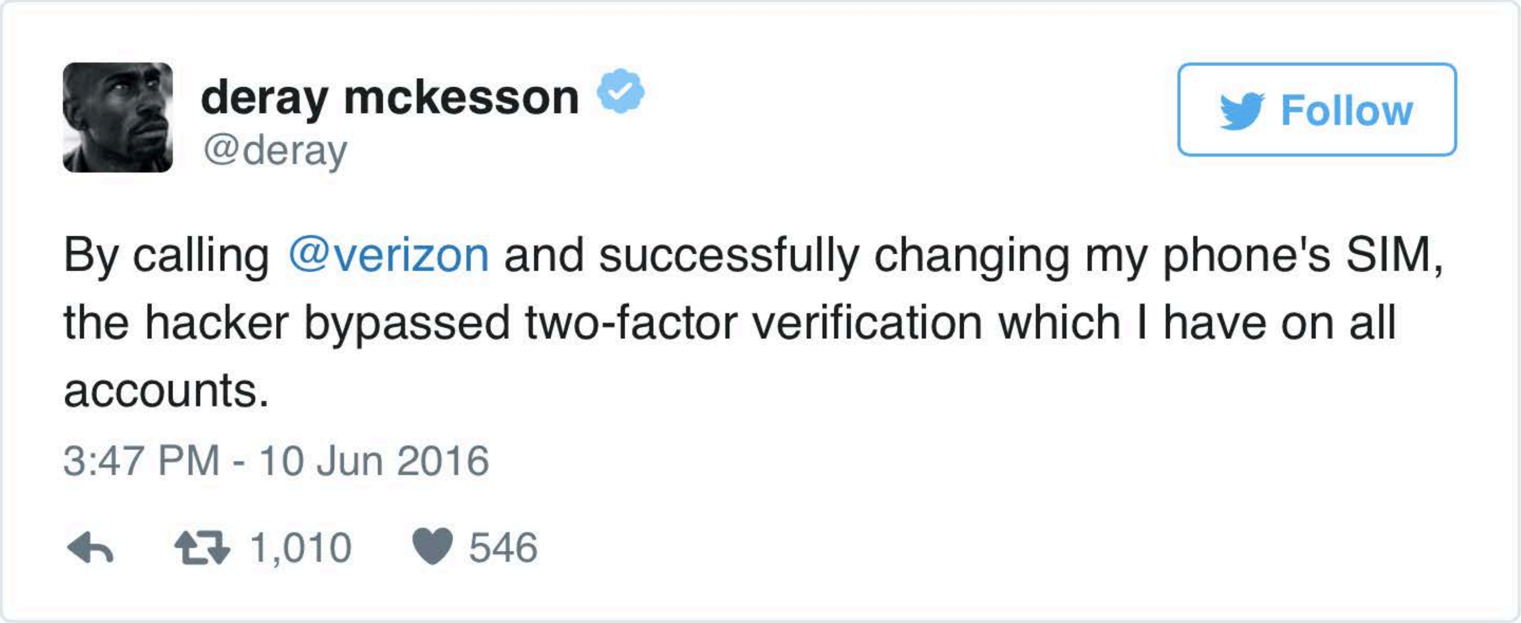


deray mckesson
@deray

At 10:31 am, someone called @verizon impersonating me and successfully changed my SIM & unsuccessfully attempted to change my phone number.

3:46 PM - 10 Jun 2016

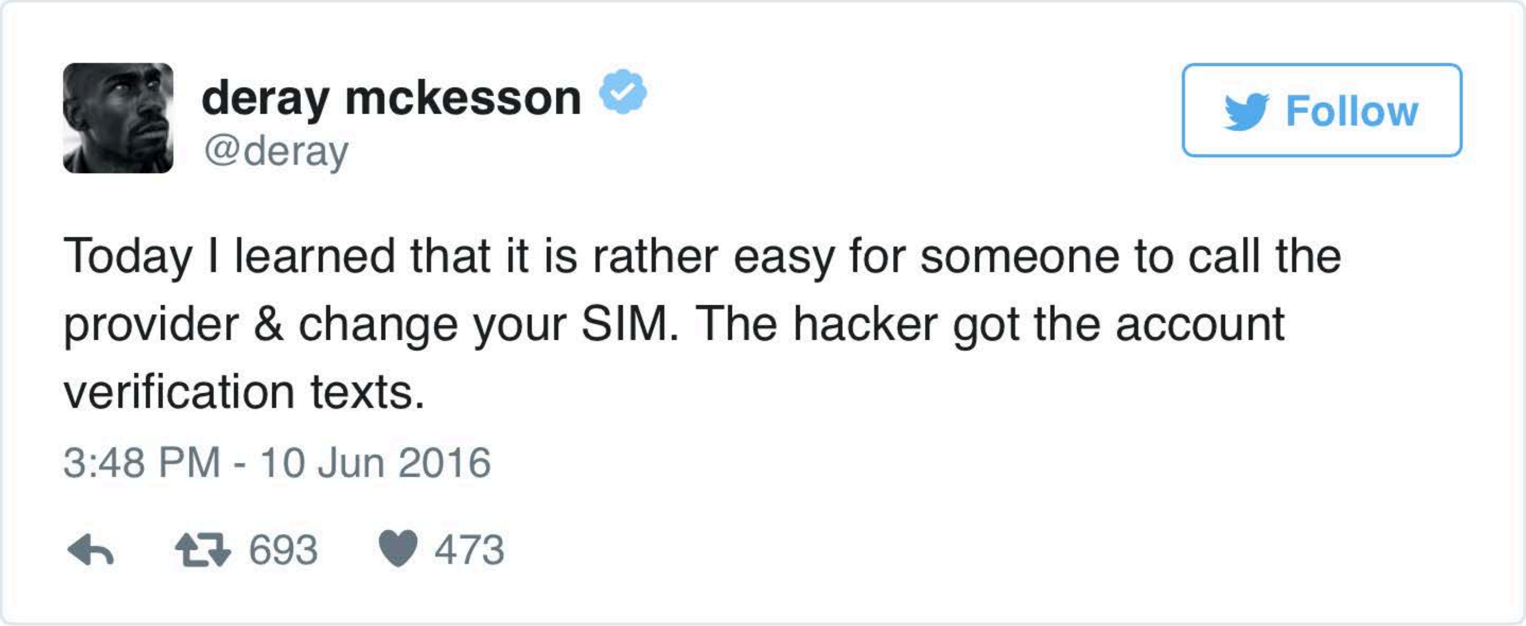
736 411



deray mckesson
@deray

By calling @verizon and successfully changing my phone's SIM, the hacker bypassed two-factor verification which I have on all accounts.

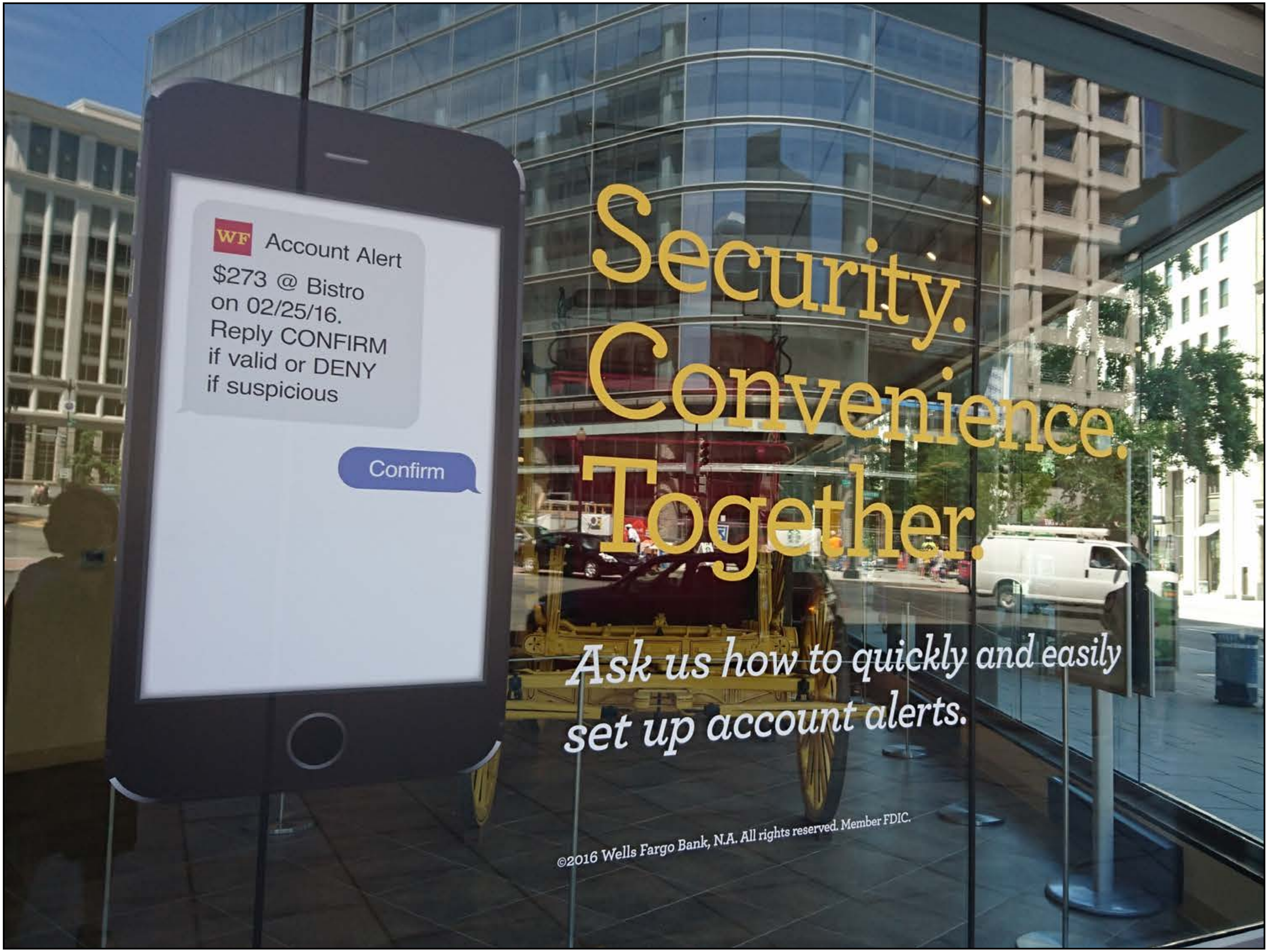
3:47 PM - 10 Jun 2016



deray mckesson
@deray

Today I learned that it is rather easy for someone to call the provider & change your SIM. The hacker got the account verification texts.

3:48 PM - 10 Jun 2016



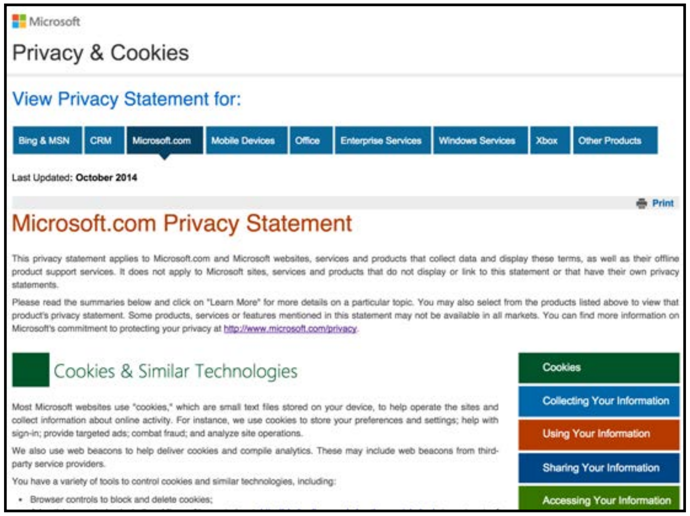
WF Account Alert

$273 @ Bistro on 02/25/16. Reply CONFIRM if valid or DENY if suspicious

Confirm

Ask us how to quickly and easily set up account alerts.

Disclosures



Microsoft

Privacy & Cookies

View Privacy Statement for:

Last Updated: **October 2014**

Microsoft.com Privacy Statement

This privacy statement applies to Microsoft.com and Microsoft websites, services and products that collect data and display these terms, as well as their offline product support services. It does not apply to Microsoft sites, services and products that do not display or link to this statement or that have their own privacy statements.

Please read the summaries below and click on "Learn More" for more details on a particular topic. You may also select from the products listed above to view that product's privacy statement. Some products, services or features mentioned in this statement may not be available in all markets. You can find more information on Microsoft's commitment to protecting your privacy at http://www.microsoft.com/privacy.

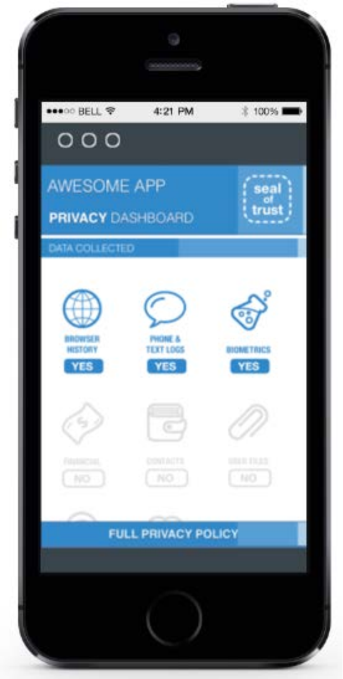
Cookies & Similar Technologies

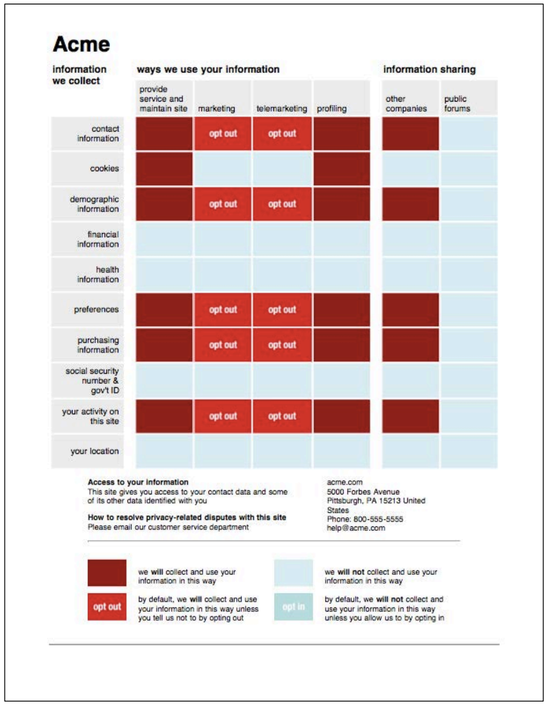
Most Microsoft websites use "cookies," which are small text files stored on your device, to help operate the sites and collect information about online activity. For instance, we use cookies to store your preferences and settings; help with sign-in; provide targeted ads; combat fraud; and analyze site operations.

We also use web beacons to help deliver cookies and compile analytics. These may include web beacons from third-party service providers.

You have a variety of tools to control cookies and similar technologies, including:

- Browser controls to block and delete cookies;





Acme

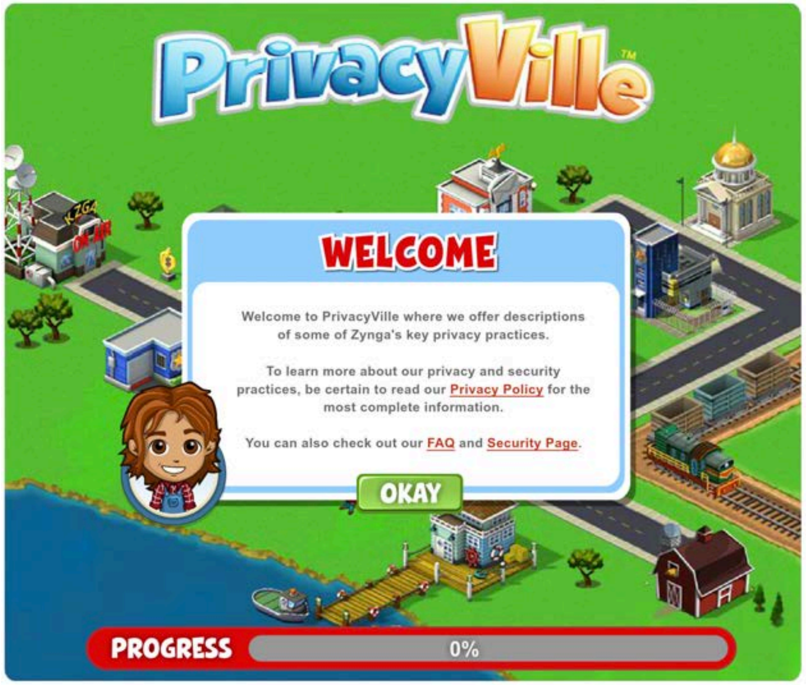
information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information	■	opt out	opt out	■	■	□
cookies	■	□	□	■	□	□
demographic information	■	opt out	opt out	■	■	□
financial information	□	□	□	□	□	□
health information	□	□	□	□	□	□
preferences	■	opt out	opt out	■	■	□
purchasing information	■	opt out	opt out	■	■	□
social security number & gov't ID	□	□	□	□	□	□
your activity on this site	■	opt out	opt out	■	■	□
your location	□	□	□	□	□	□

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

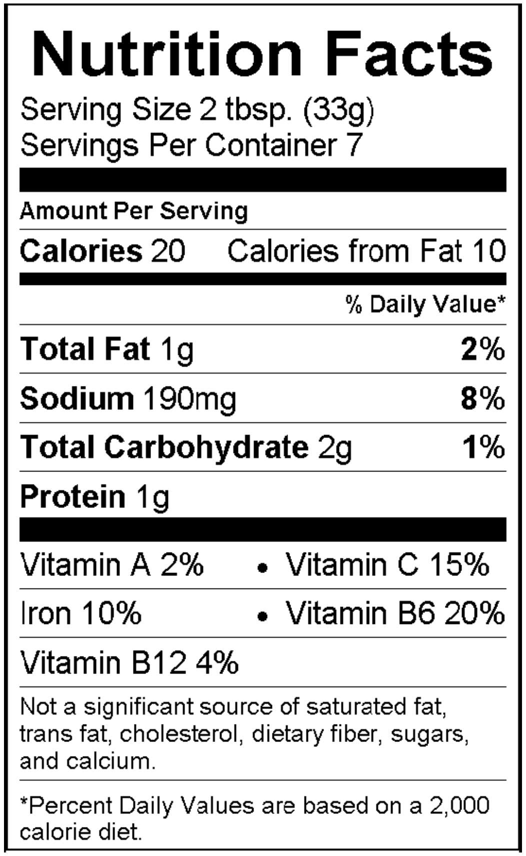
■	we **will** collect and use your information in this way
opt out	by default, we **will** collect and use your information in this way unless you tell us not to by opting out
□	we **will not** collect and use your information in this way
opt in	by default, we **will not** collect and use your information in this way unless you allow us to by opting in



Welcome to PrivacyVille where we offer descriptions of some of Zynga's key privacy practices.

To learn more about our privacy and security practices, be certain to read our Privacy Policy for the most complete information.

You can also check out our FAQ and Security Page.



Nutrition Facts

Serving Size 2 tbsp. (33g)
Servings Per Container 7

Amount Per Serving

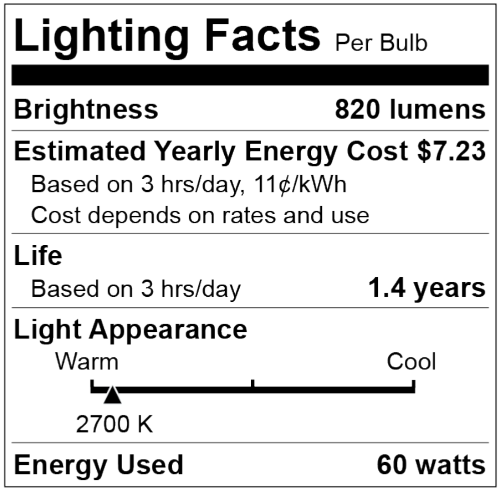
Calories 20 Calories from Fat 10

	% Daily Value*
Total Fat 1g	**2%**
Sodium 190mg	**8%**
Total Carbohydrate 2g	**1%**
Protein 1g	

Vitamin A 2%	• Vitamin C 15%
Iron 10%	• Vitamin B6 20%
Vitamin B12 4%	

Not a significant source of saturated fat, trans fat, cholesterol, dietary fiber, sugars, and calcium.

*Percent Daily Values are based on a 2,000 calorie diet.



Lighting Facts Per Bulb

Brightness	**820 lumens**
Estimated Yearly Energy Cost	**$7.23**

Based on 3 hrs/day, 11¢/kWh
Cost depends on rates and use

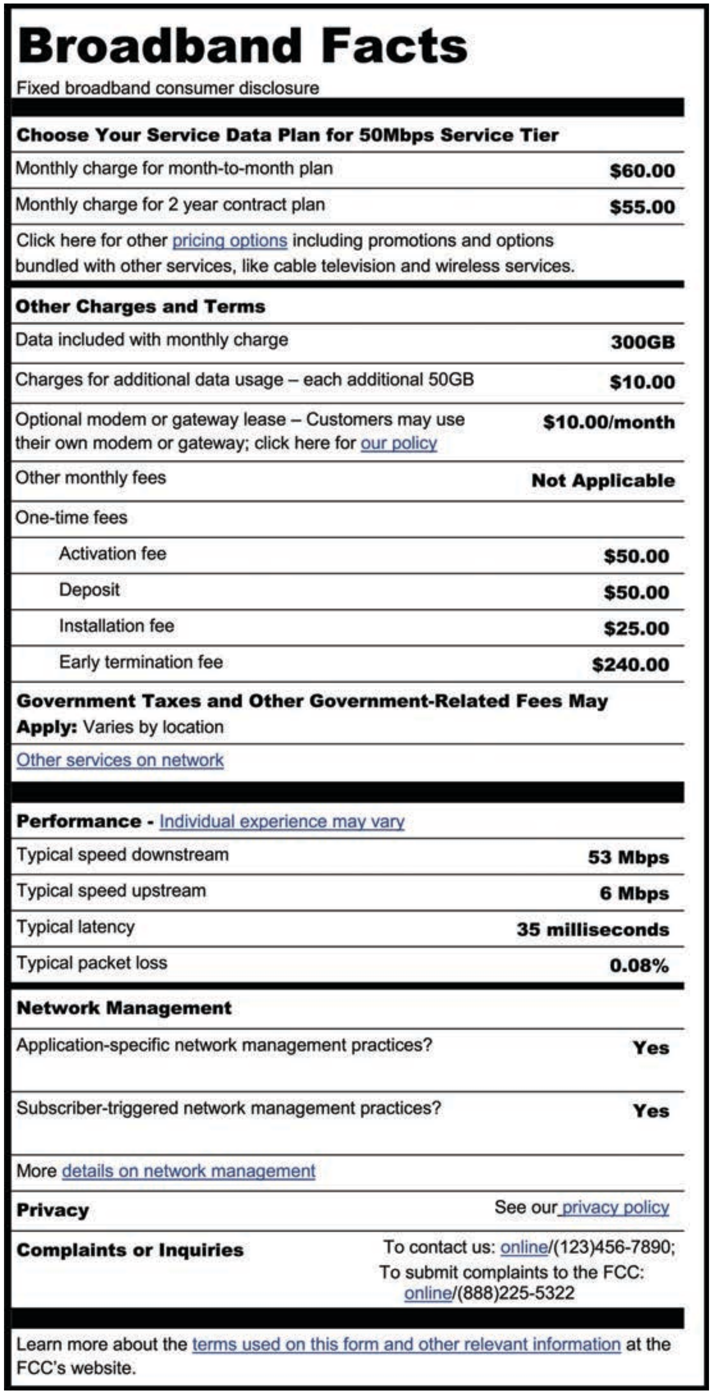
Life

Based on 3 hrs/day	**1.4 years**

Light Appearance

Warm
Cool
2700 K

Energy Used	**60 watts**



Broadband Facts

Fixed broadband consumer disclosure

Choose Your Service Data Plan for 50Mbps Service Tier

Monthly charge for month-to-month plan	**$60.00**
Monthly charge for 2 year contract plan	**$55.00**

Click here for other pricing options including promotions and options bundled with other services, like cable television and wireless services.

Other Charges and Terms

Data included with monthly charge	**300GB**
Charges for additional data usage – each additional 50GB	**$10.00**
Optional modem or gateway lease – Customers may use their own modem or gateway; click here for our policy	**$10.00/month**
Other monthly fees	**Not Applicable**
One-time fees	
Activation fee	**$50.00**
Deposit	**$50.00**
Installation fee	**$25.00**
Early termination fee	**$240.00**

Government Taxes and Other Government-Related Fees May Apply: Varies by location

Other services on network

Performance - Individual experience may vary

Typical speed downstream	**53 Mbps**
Typical speed upstream	**6 Mbps**
Typical latency	**35 milliseconds**
Typical packet loss	**0.08%**

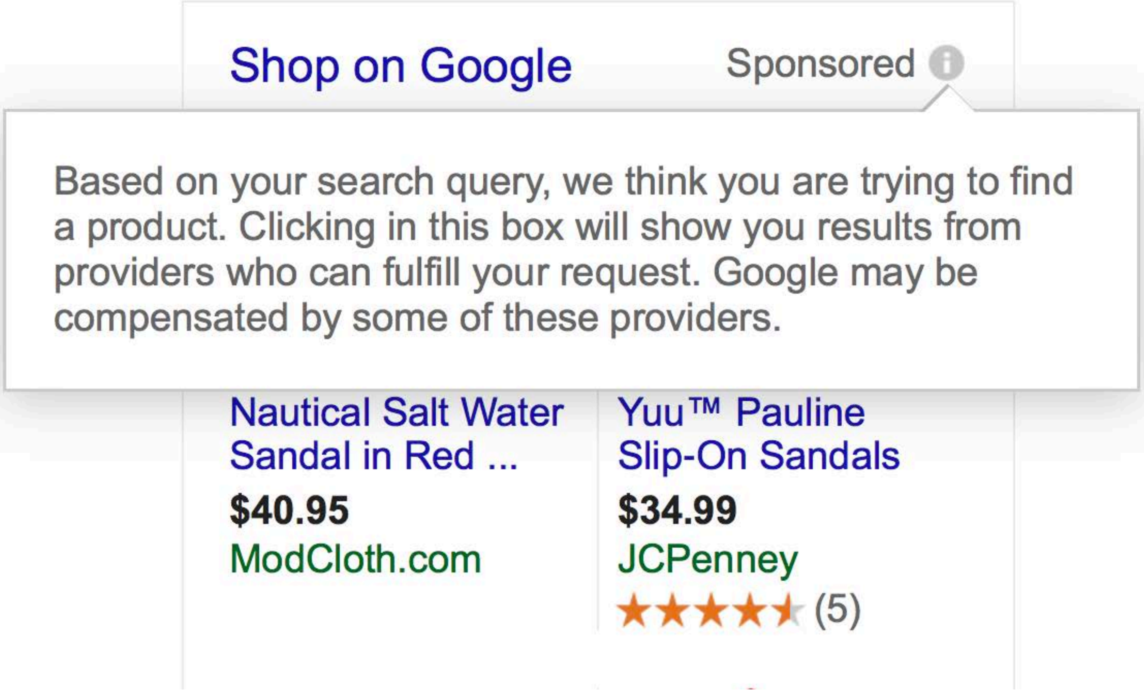
Network Management

Application-specific network management practices?	**Yes**
Subscriber-triggered network management practices?	**Yes**

More details on network management

Privacy	See our privacy policy
Complaints or Inquiries	To contact us: online/(123)456-7890; To submit complaints to the FCC: online/(888)225-5322

Learn more about the terms used on this form and other relevant information at the FCC's website.



Shop on Google

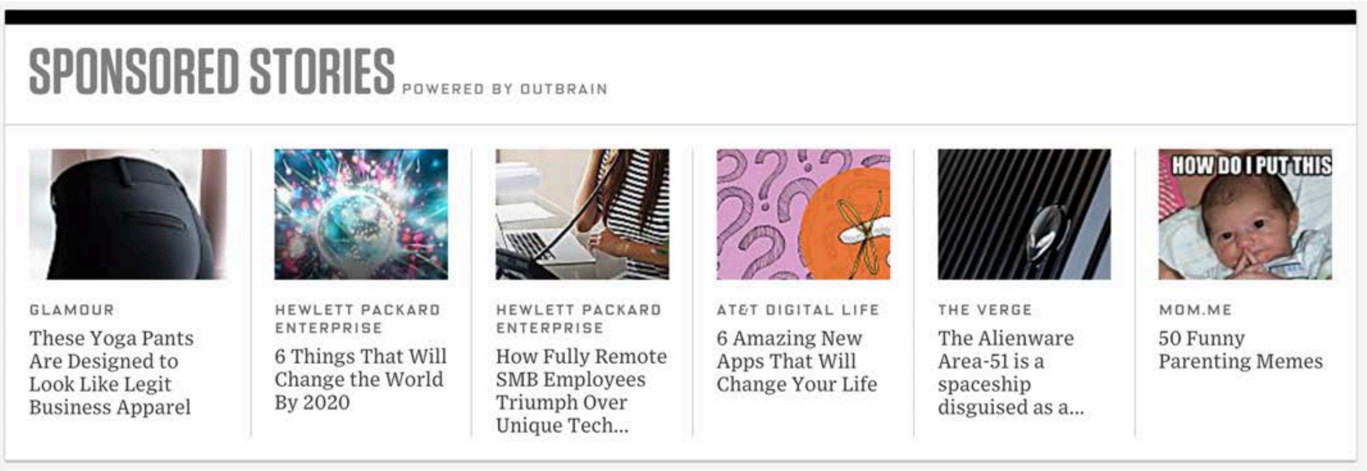
Sponsored

Based on your search query, we think you are trying to find a product. Clicking in this box will show you results from providers who can fulfill your request. Google may be compensated by some of these providers.

Nautical Salt Water Sandal in Red ...
$40.95
ModCloth.com

Yuu™ Pauline Slip-On Sandals
$34.99
JCPenney
★★★★★ (5)

WASH WITH SIMILAR COLOURS,
WASH INSIDE OUT,
WASH AS WOOL CYCLE,
DO NOT PILE WHILST DAMP,



SPONSORED STORIES POWERED BY OUTBRAIN

GLAMOUR
These Yoga Pants Are Designed to Look Like Legit Business Apparel

HEWLETT PACKARD ENTERPRISE
6 Things That Will Change the World By 2020

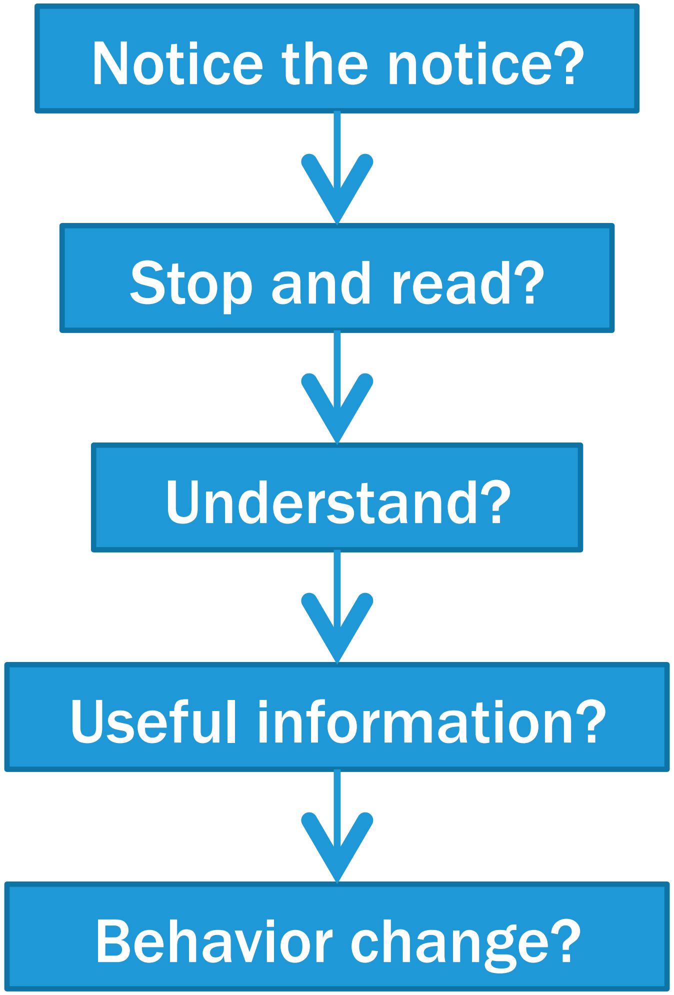
HEWLETT PACKARD ENTERPRISE
How Fully Remote SMB Employees Triumph Over Unique Tech...

AT&T DIGITAL LIFE
6 Amazing New Apps That Will Change Your Life

THE VERGE
The Alienware Area-51 is a spaceship disguised as a...

MOM.ME
50 Funny Parenting Memes

By what criteria should we measure effectiveness?



Notice the notice?

Stop and read?

Understand?

Useful information?

Behavior change?

Role of mediators?

FTC Workshop: Putting Disclosures to the Test

- September 15, 2016, Washington, DC
- We want to hear about your experiences testing and evaluating disclosures
  - Emphasis on evaluation methods and lessons learned
- Email proposal to present by July 15, 2016
- See ftc.gov/tech

The FTC wants to hear about your research!

Participate in FTC events

- Ransomware workshop – September 7
- Drones workshop – October 13
- SmartTV workshop – December 7
- PrivacyCon – January 12

Serge Egelman
University of California, Berkeley

Android Permissions Remystified: A Field Study on Contextual Integrity

Co-authors: Primal Wijesekera (University of British Columbia); Arjun Baokar, Ashkan Hosseini, David Wagner (University of California, Berkeley); Konstantin Beznosov (University of British Columbia)

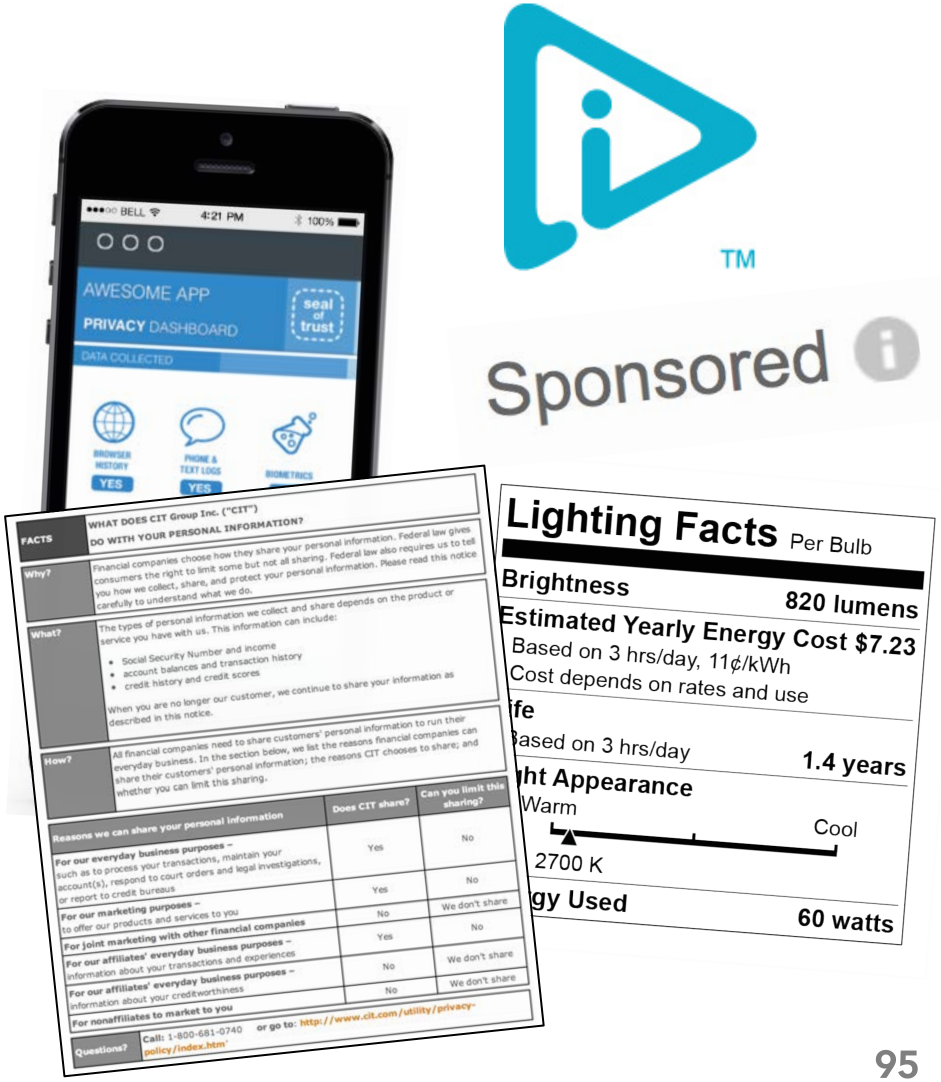
FTC interest in SOUPS-related research

- Disclosures and labeling
- Understanding and quantifying privacy and security
- Investigation and enforcement
- Consumer and business education

- Ads and marketing
- Financial technologies
- Every community
- Anti-trust
- Tools and techniques
- Emerging technologies and trends

Disclosures and labeling

- How to evaluate?
- Pros and cons of short notices, icons, etc?
- User perceptions?
- Influence on behavior?
- Use of automation?
- Role of mediators?



FACTS	WHAT DOES CIT Group Inc. ("CIT") DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depends on the product or service you have with us. This information can include: • Social Security Number and income • account balances and transaction history • credit history and credit scores When you are no longer our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons CIT chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does CIT share?	Can you limit this sharing?
For our everyday business purposes – such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes – information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	**Call:** 1-800-681-0740 **or go to:** http://www.cit.com/utility/privacy-policy/index.htm'

Lighting Facts Per Bulb

Brightness	**820 lumens**
Estimated Yearly Energy Cost	**$7.23**
Based on 3 hrs/day, 11¢/kWh Cost depends on rates and use	
ife	
3ased on 3 hrs/day	**1.4 years**
ght Appearance	
Warm — Cool 2700 K	
gy Used	**60 watts**

Understanding and quantifying privacy and security

- How do consumers value aspects of privacy?
- What are privacy expectations and concerns in various contexts?
- Impact of information exposure?
- How to assess risk of harm related to security and privacy breaches?
- How do consumers balance privacy against benefits from data?
- Attack trends and responses

Investigation and enforcement

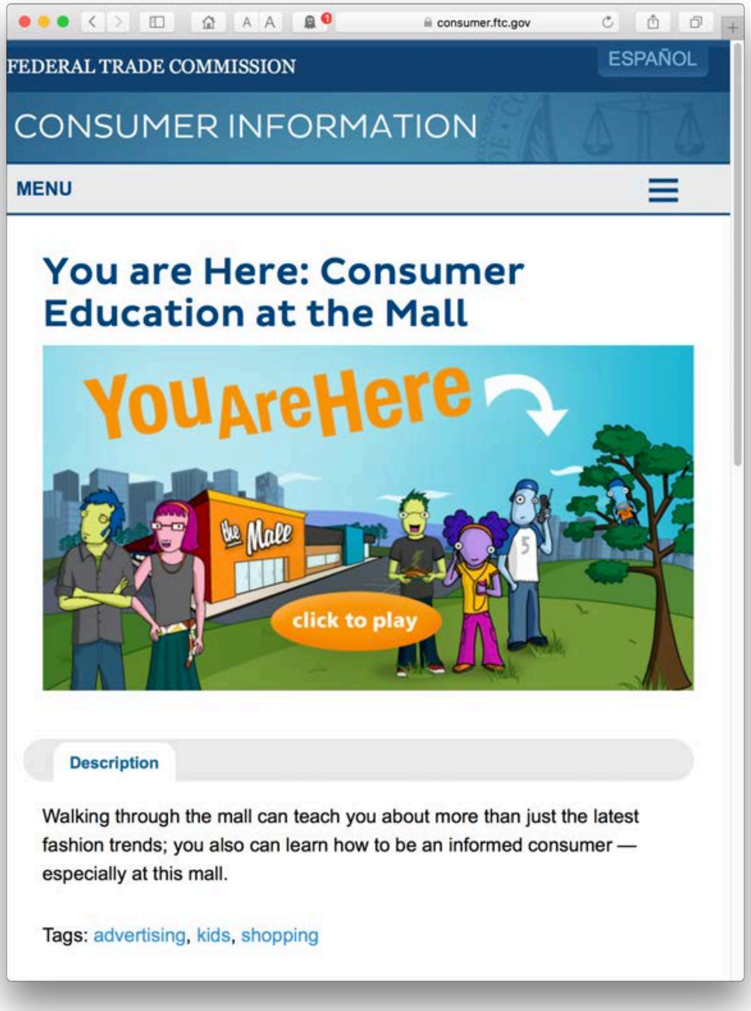
- How can the FTC encourage consumers to report fraud, scams, unwanted calls?
- How can the FTC improve UI for complaint reporting?
- How can the FTC assess self-selection bias in consumer complaints?

Consumer and business education

- How can the FTC measure behavior change as the result of an educational campaign or intervention?

- How usable, informative, and engaging are FTC education materials? How can they be improved?

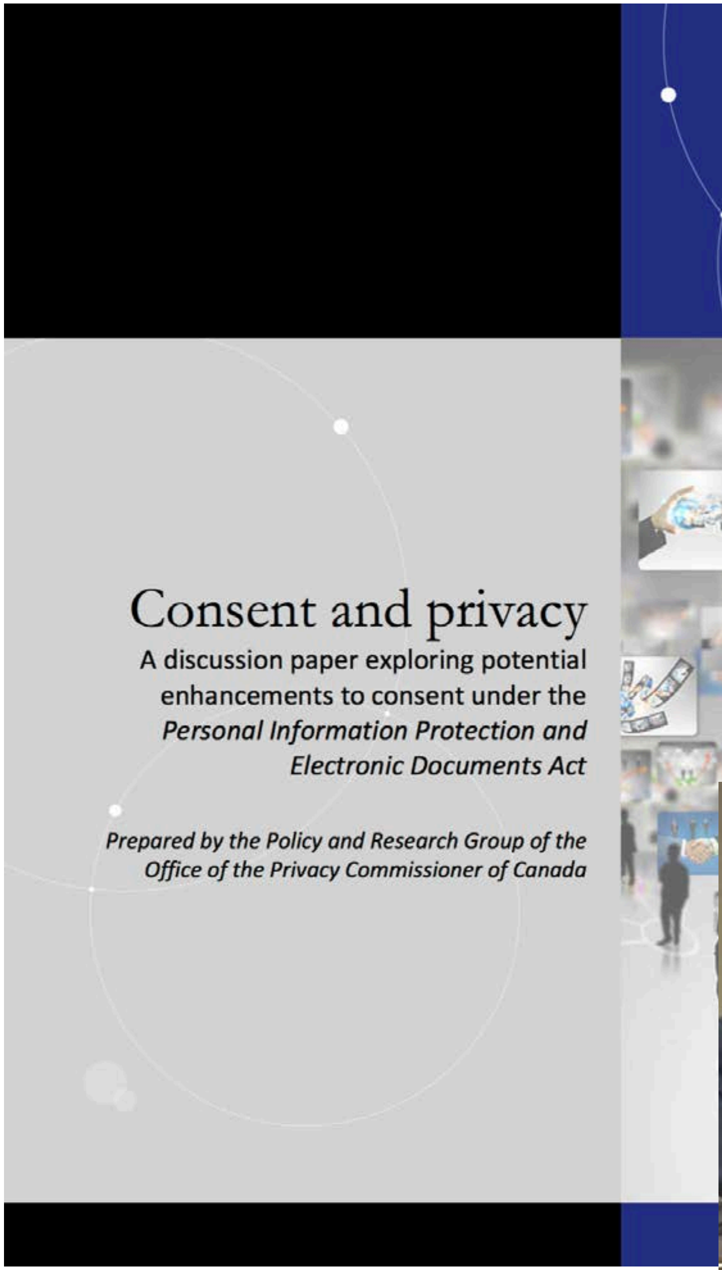
- How can the FTC better educate consumers to identify well-known signs of fraud?



You are Here: Consumer Education at the Mall

Walking through the mall can teach you about more than just the latest fashion trends; you also can learn how to be an informed consumer — especially at this mall.

Tags: advertising, kids, shopping



Office of the Privacy Commissioner of Canada

Consent and privacy

A discussion paper exploring potential enhancements to consent under the *Personal Information Protection and Electronic Documents Act*

Prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada

Canadian?

Privacy Commissioner wants feedback on consent and privacy

Responses due July 13, 2016

Public policy contributions

CHI 2017

EXPLORE INNOVATE INSPIRE

Understanding policy impacts

- Impacts of law or policy on people
- Impacts of a technology or design on a policy goal

SOUPS
Symposium On Usable Privacy and Security
2016

ftc.gov/tech

lcranor @ ftc.gov