Hearing #9 on Competition and Consumer Protection in the 21st Century

Constitution Center

December 11, 2018

Welcome
We Will Be Starting Shortly

Welcome and Introductory Remarks

Elisa Jillson

Federal Trade Commission

Division of Privacy and Identity Protection

Opening Remarks

Andrew Smith
Federal Trade Commission
Bureau of Consumer Protection

Presentations on Data Breaches

2018 Data Breach Investigations Report

Marc Spitler

Strategic News Bundling and Privacy Breach Disclosures

Sebastien Gay

2018 Identity Fraud: Fraud Enters a New Era of Complexity

Al Pascual

Moderators: Jared Ho, Marc Luppino

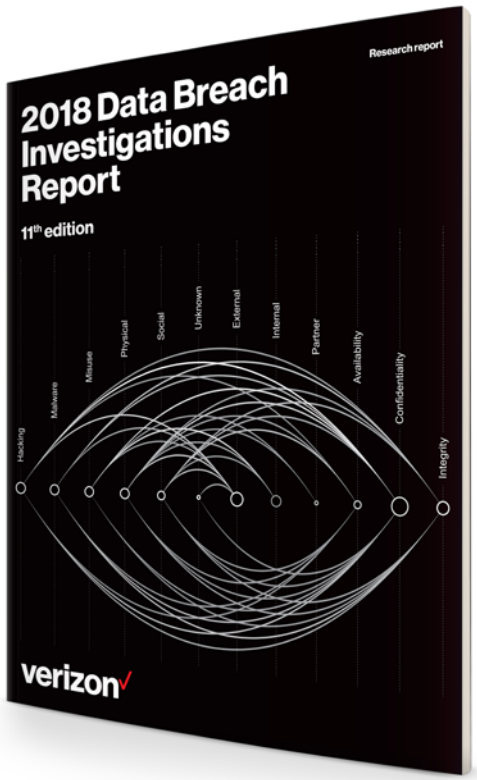
2018 Data Breach Investigations Report

verizon

Hearings on Competition and Consumer Protection in the 21st Century
An FTC Event | December 11-12, 2018 | ftc.gov/ftc-hearings | #ftchearings

Facts versus opinions.

11th edition	:	**2,216** breaches	**53,308** incidents
Last 5 years	:	**9,900** breaches	**302,802** incidents
Corpus	:	**16k+** breaches	**330k+** incidents



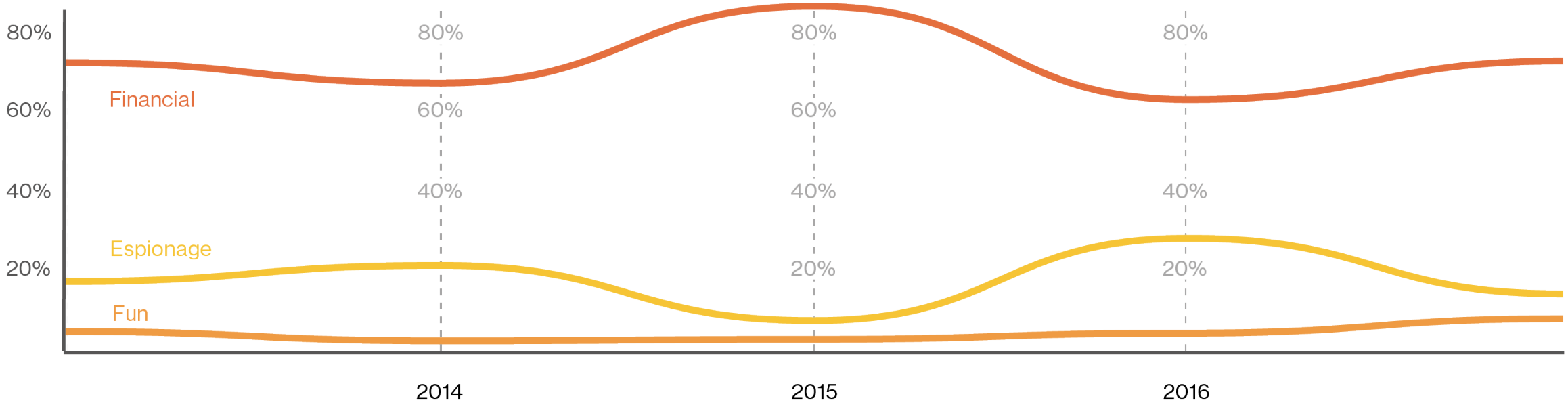
DBIR is based on analysis of real world security incidents and confirmed data breaches.

Information is supplied by 67 partners in the latest edition, covering 1000s of companies in 65 countries.

verizon

Show me the money.

The motive behind most breaches is money.

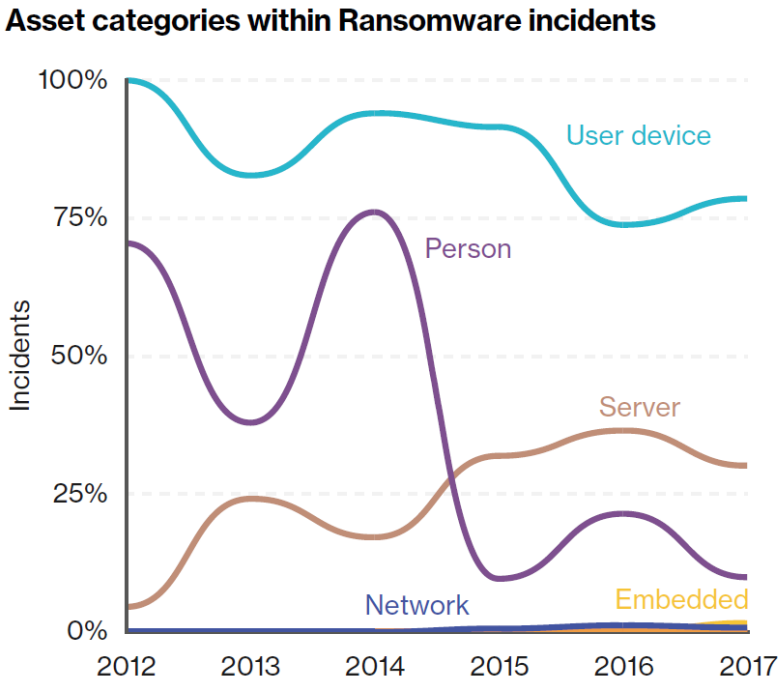


verizon

Ransomware

If you ever want to see your precious data again…

We hate being right – back in 2013 we said: “[This may] blossom as an effective tool of choice for online criminals”



- Doubled again this year after having doubled last year.
- Responsible for 39% of all malware related breaches.
- Ransomware accounts for 85% of all malware in Healthcare.

verizon

Social Engineering

We're only human

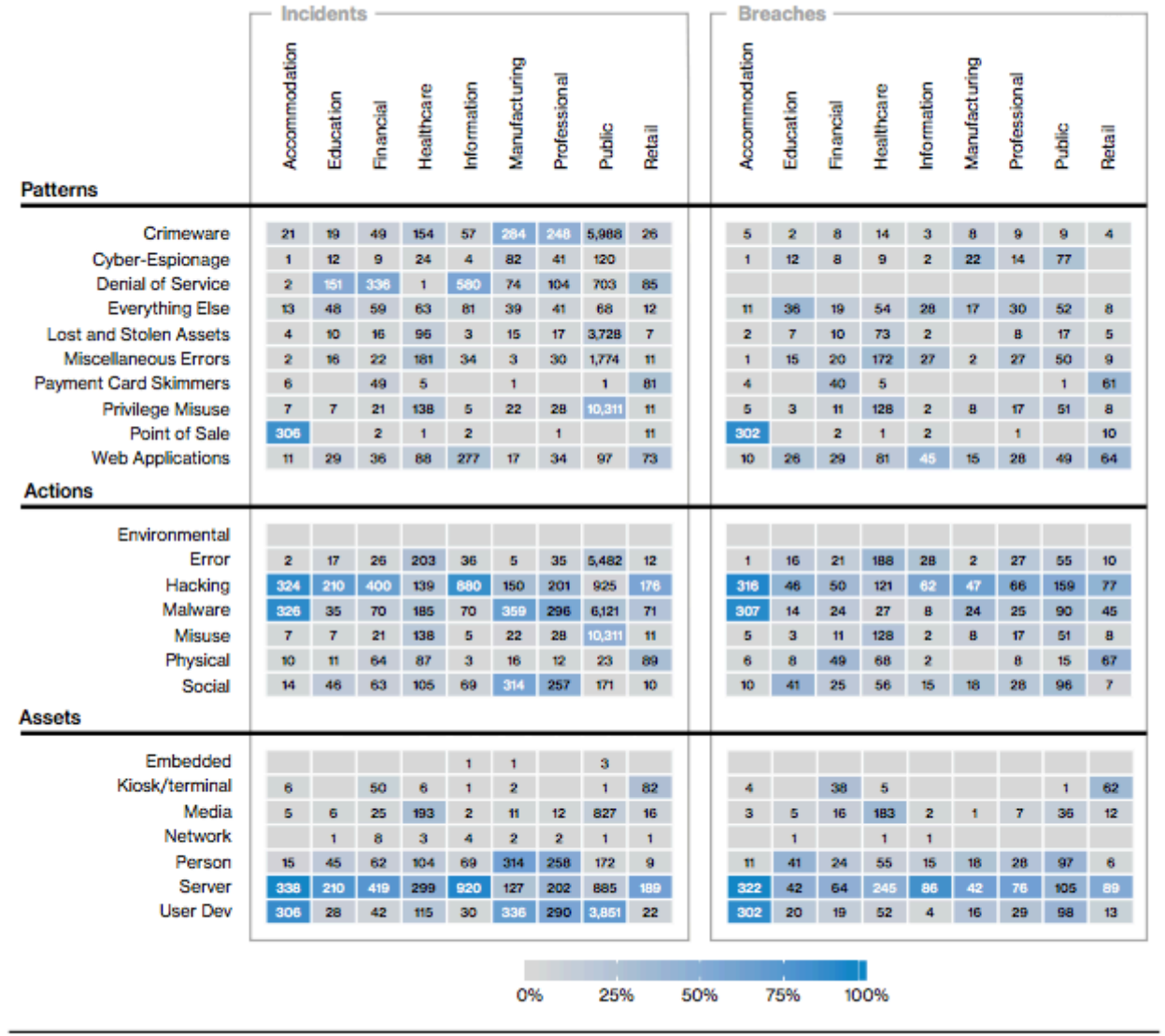
Frequency	1,450 incidents, 381 with confirmed data disclosure
Top 3 patterns	Crimeware, Everything Else, and Cyber-Espionage represent 93% of all security incidents
Threat actors	99% External, 6% Internal, <1% Partner (breaches)
Actor motives	59% Financial, 38% Espionage (breaches)
Data compromised	47% Personal, 26% Secrets, 22% Internal, 17% Credentials

Phishing and pretexting represent 98% of social incidents and 93% of breaches.

verizon

Vertical differences

The table shows how different the breakouts of actors, motives, tactics, and attack patterns look across industries.
Some industries handle significant amounts of payment card data, some have databases full to the brim with personally identifiable information (PII), some protect classified information and some
are lucky enough to do all of the above.



	Incidents									Breaches								
Patterns	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail	Accommodation	Education	Financial	Healthcare	Information	Manufacturing	Professional	Public	Retail
Crimeware	21	19	49	154	57	284	248	5,988	26	5	2	8	14	3	8	9	9	4
Cyber-Espionage	1	12	9	24	4	82	41	120		1	12	8	9	2	22	14	77	
Denial of Service	2	151	336	1	580	74	104	703	85									
Everything Else	13	48	59	63	81	39	41	68	12	11	36	19	54	28	17	30	52	8
Lost and Stolen Assets	4	10	16	95	3	15	17	3,728	7	2	7	10	73	2		8	17	5
Miscellaneous Errors	2	16	22	181	34	3	30	1,774	11	1	15	20	172	27	2	27	50	9
Payment Card Skimmers	6		49	5		1		1	81	4		40	5				1	61
Privilege Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Point of Sale	306		2	1	2		1		11	302		2	1	2		1		10
Web Applications	11	29	36	88	277	17	34	97	73	10	26	29	81	45	15	28	49	64
Actions																		
Environmental																		
Error	2	17	26	203	36	5	35	5,482	12	1	16	21	188	28	2	27	55	10
Hacking	324	210	400	139	880	150	201	925	176	316	46	50	121	62	47	66	159	77
Malware	326	35	70	185	70	359	296	6,121	71	307	14	24	27	8	24	25	90	45
Misuse	7	7	21	138	5	22	28	10,311	11	5	3	11	128	2	8	17	51	8
Physical	10	11	64	87	3	16	12	23	89	6	8	49	68	2		8	15	67
Social	14	46	63	105	69	314	257	171	10	10	41	25	56	15	18	28	96	7
Assets																		
Embedded					1	1		3										
Kiosk/terminal	6		50	6	1	2		1	82	4		38	5				1	62
Media	5	6	25	193	2	11	12	827	16	3	5	16	183	2	1	7	36	12
Network		1	8	3	4	2	2	1	1		1		1	1				
Person	15	45	62	104	69	314	258	172	9	11	41	24	55	15	18	28	97	6
Server	338	210	419	299	920	127	202	885	189	322	42	64	245	86	42	76	105	89
User Dev	306	28	42	115	30	336	290	3,851	22	302	20	19	52	4	16	29	98	13

0% 25% 50% 75% 100%

Figure 28. Industry comparison (left: all security incidents, right: only confirmed data breaches)

verizon

Threat Action Varieties

- Denial of Service attacks are common across numerous industries for incidents.
- Use of stolen creds and social attack related breaches plague several verticals.
- Privilege Abuse rampant in Public and Healthcare.

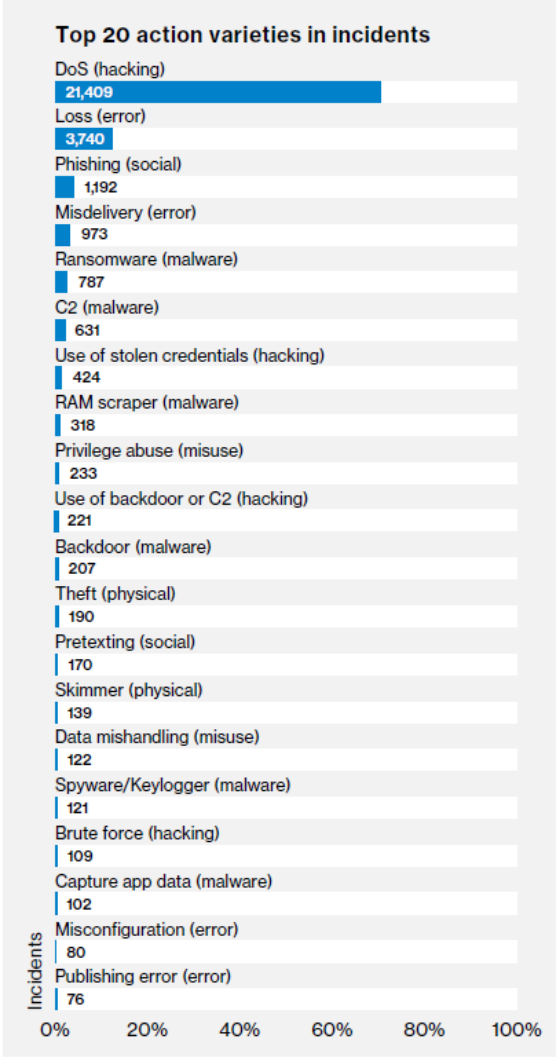


Figure 4. Top 20 threat action varieties (incidents) (n=30,362)

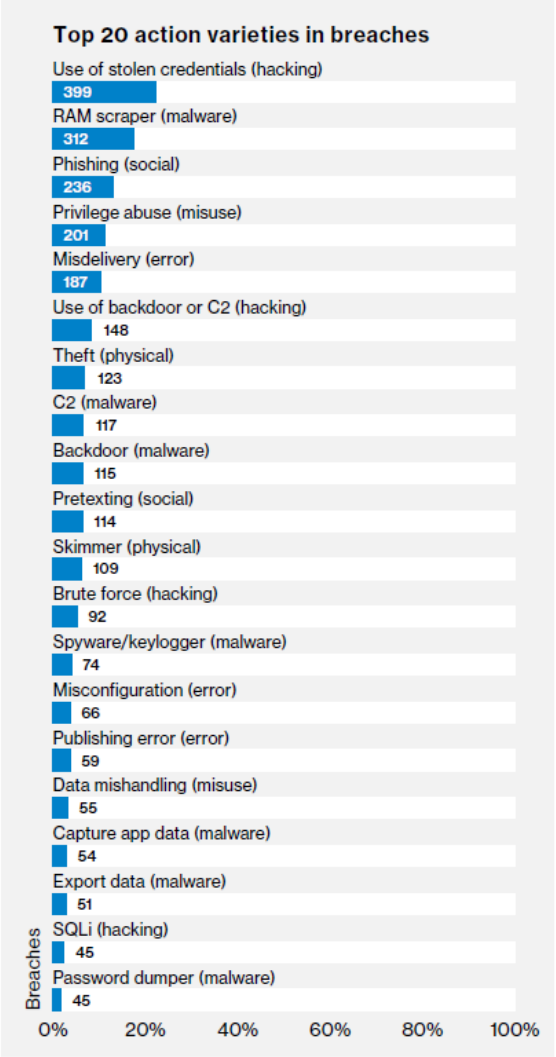


Figure 5. Top 20 threat action varieties (confirmed data breaches) (n=1,799)

verizon

Questions?

www.verizonenterprise.com/DBIR

verizon

Strategic News Bundling and Privacy Breach Disclosures

Sebastien Gay

Hearings on Competition and Consumer Protection in the 21st Century
An FTC Event | December 11-12, 2018 | ftc.gov/ftc-hearings | #ftchearings

2018 Identity Fraud Study

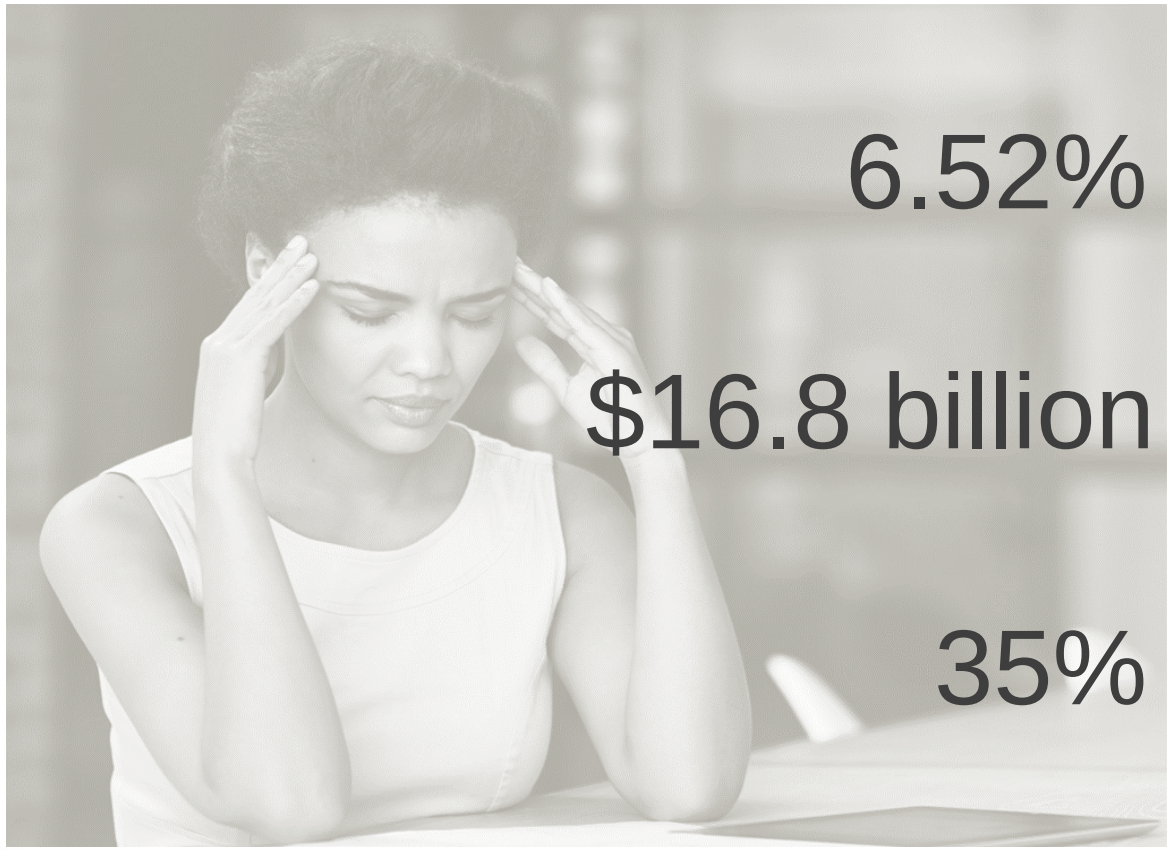
Fraud Enters a New Era of Complexity

Javelin Strategy & Research

Hearings on Competition and Consumer Protection in the 21st Century
An FTC Event | December 11-12, 2018 | ftc.gov/ftc-hearings | #ftchearings

2017 Stood Out as Fraud Became More Pervasive Than Ever and Consumers' Most Sensitive PII Was Compromised as Never Before

It was a year for the record books



Record high identity fraud incidence in 2017

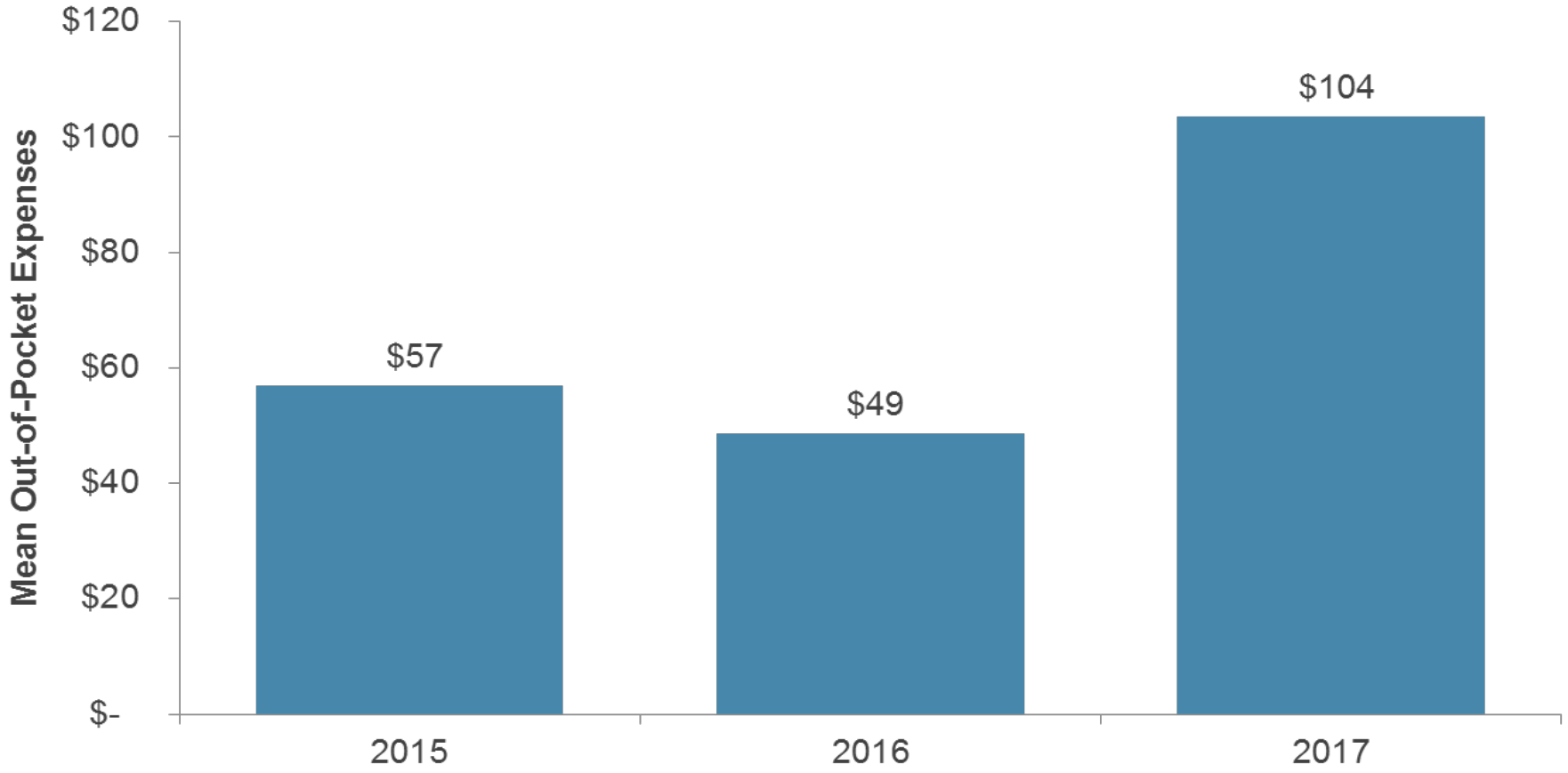
Total fraud losses at highest point in past four years

Proportion of breach victims whose SSN was compromised

Source: Javelin Strategy & Research, 2018

Victims Spent More of Their Own Money Resolving Cases of Identity Fraud in 2017

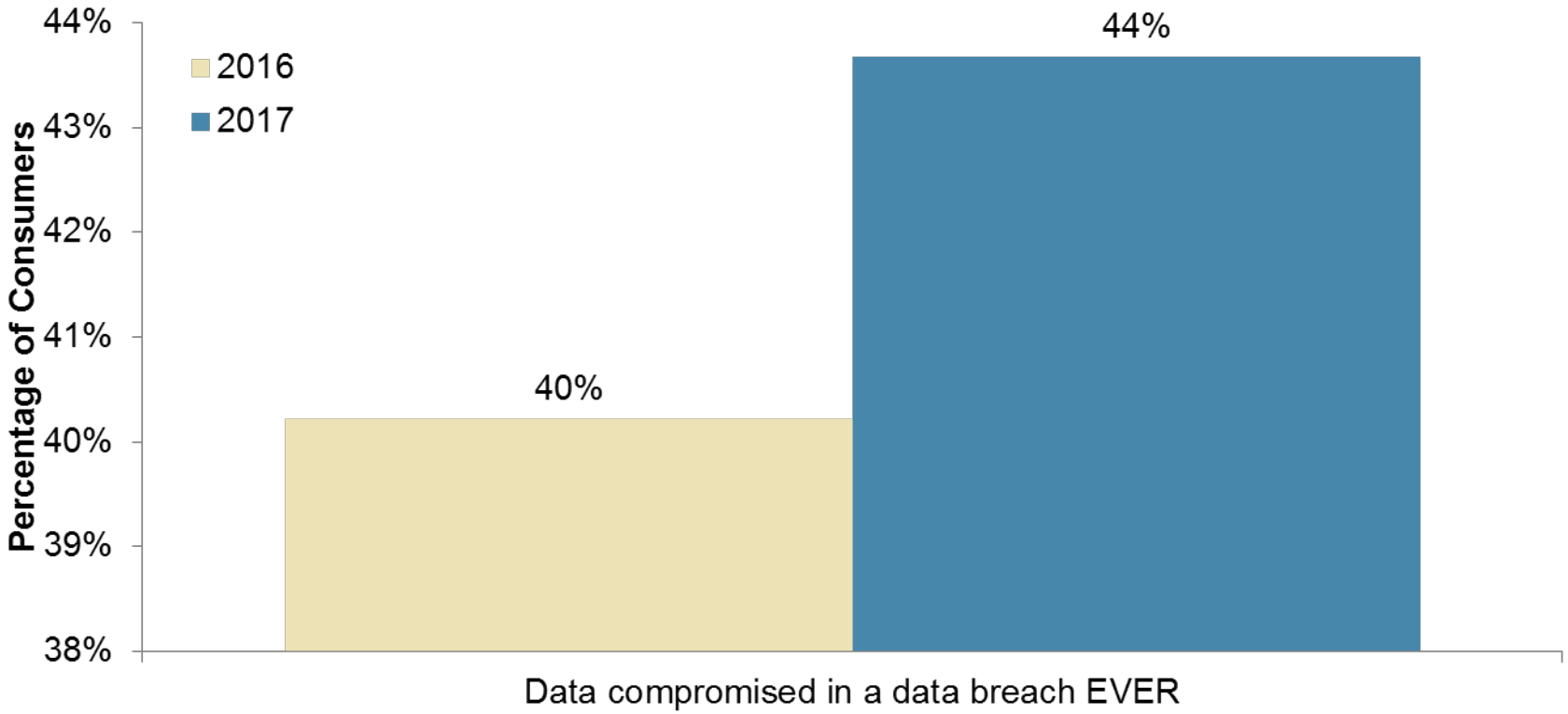
Out-of-pocket costs for victims of identity fraud, 2015-2017



Source: Javelin Strategy & Research, 2018

Nearly A Third of Consumers Hit By Data Breach in 2017, Many Not for the First Time

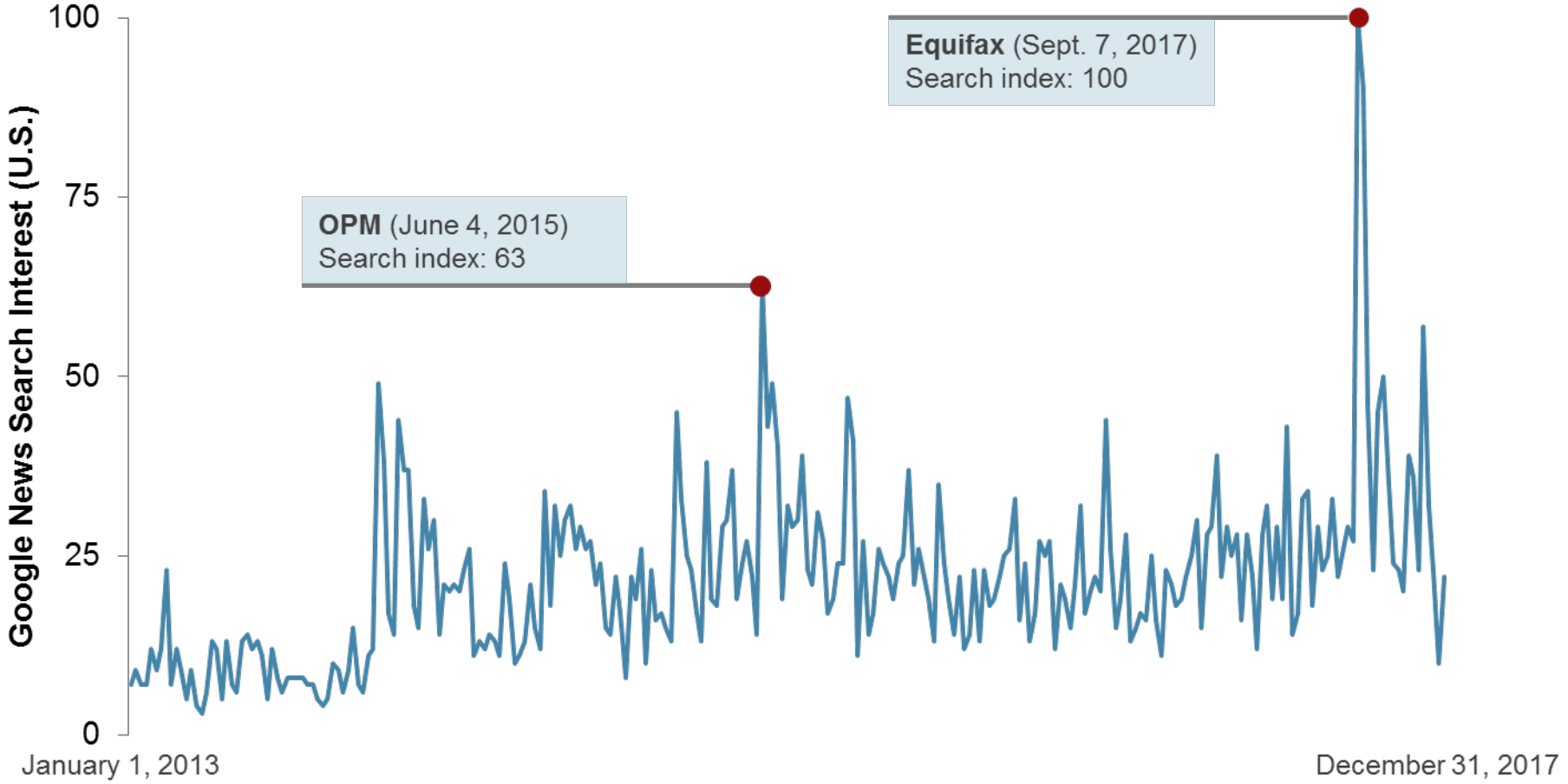
Consumers' Data Breach Status (2016-2017)



Source: Javelin Strategy & Research, 2018

The Equifax Breach Sent Consumers Scrambling for Information Wherever They Could Find It

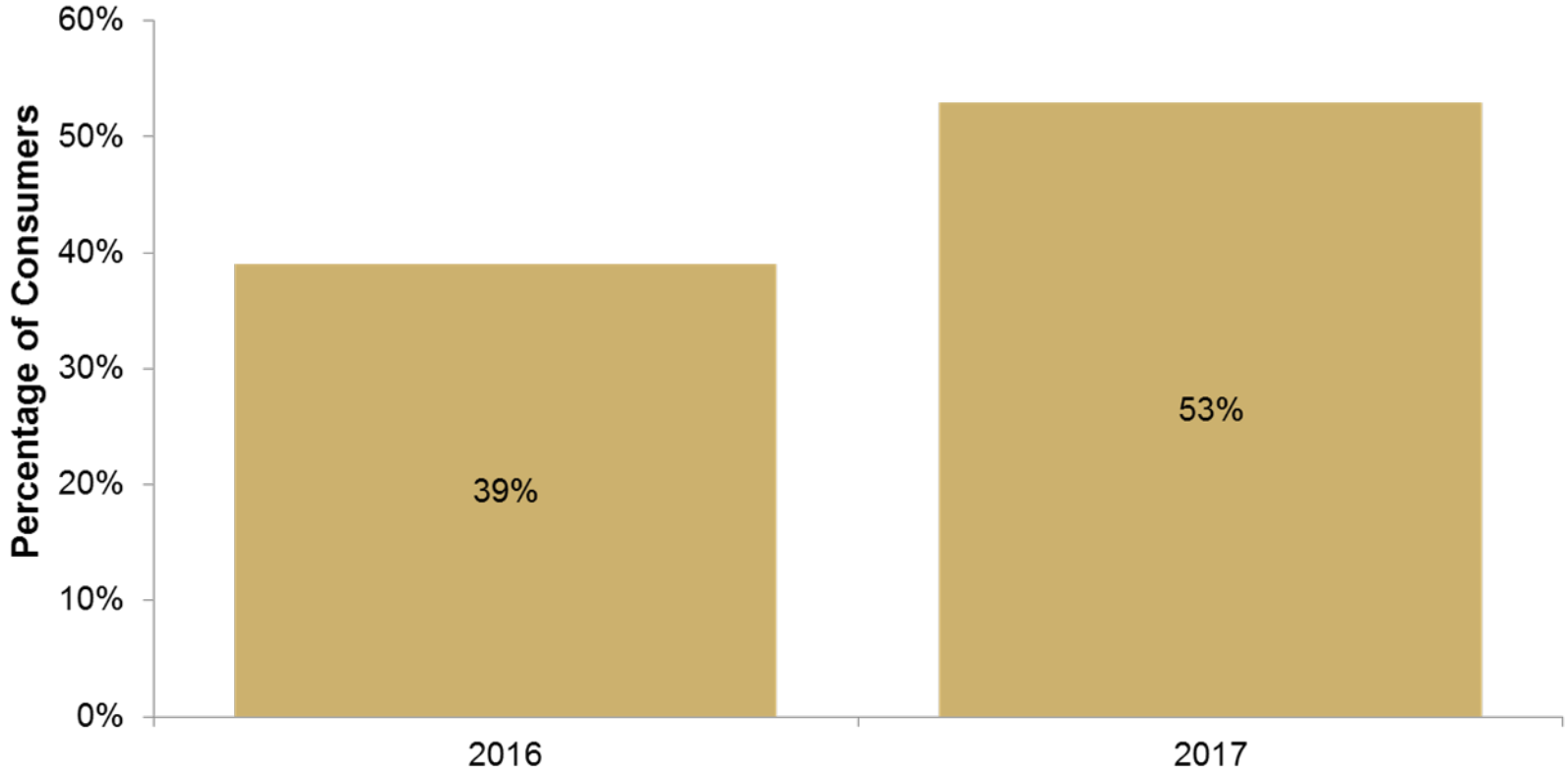
Google news search in interest “data breach” (January 2013 to December 2017)



Source: Google Trends, 2018

Cynicism Regarding Breach Notifications Understandably Jumped

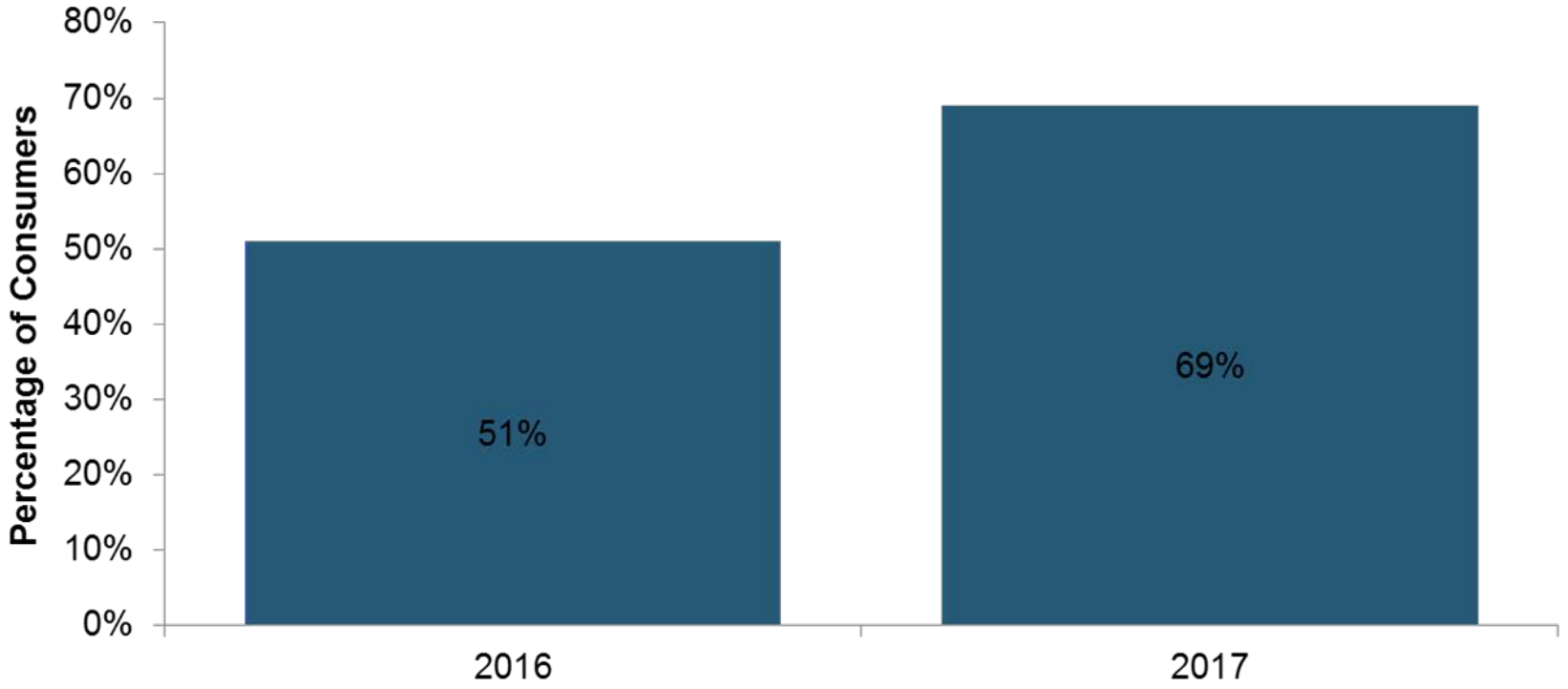
Agreement with: “Data breach notifications merely help organizations to save face or meet legal requirements, and do little to protect me”



Source: Javelin Strategy & Research, 2018

Concern About Fraud Also Rose Considerably in 2017

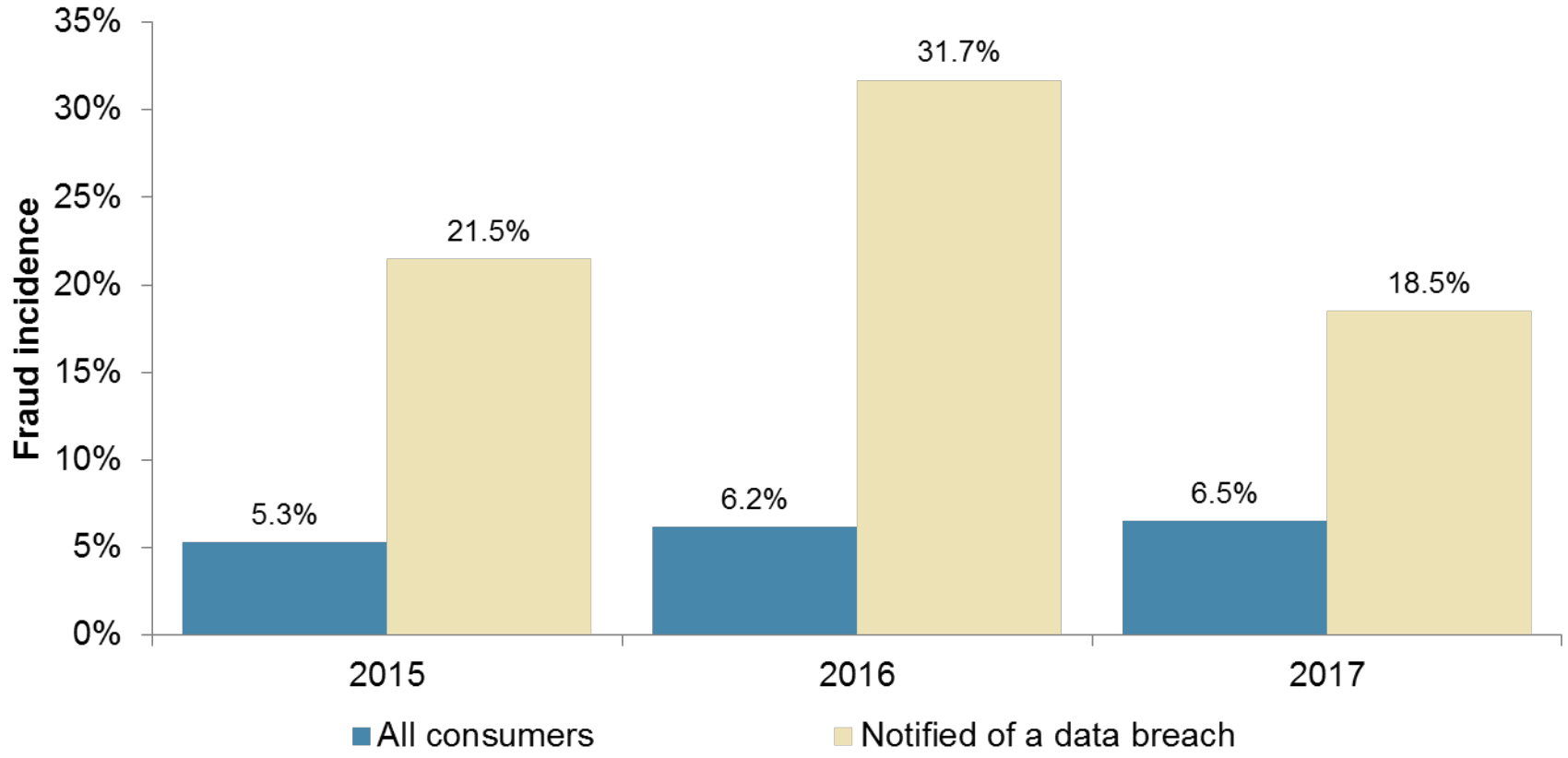
Consumers concerned about identity fraud, 2016-2017



Source: Javelin Strategy & Research, 2018

Data Breach-Fraud Connection Loosened as the Breach Population Grew and Fraud Evolved

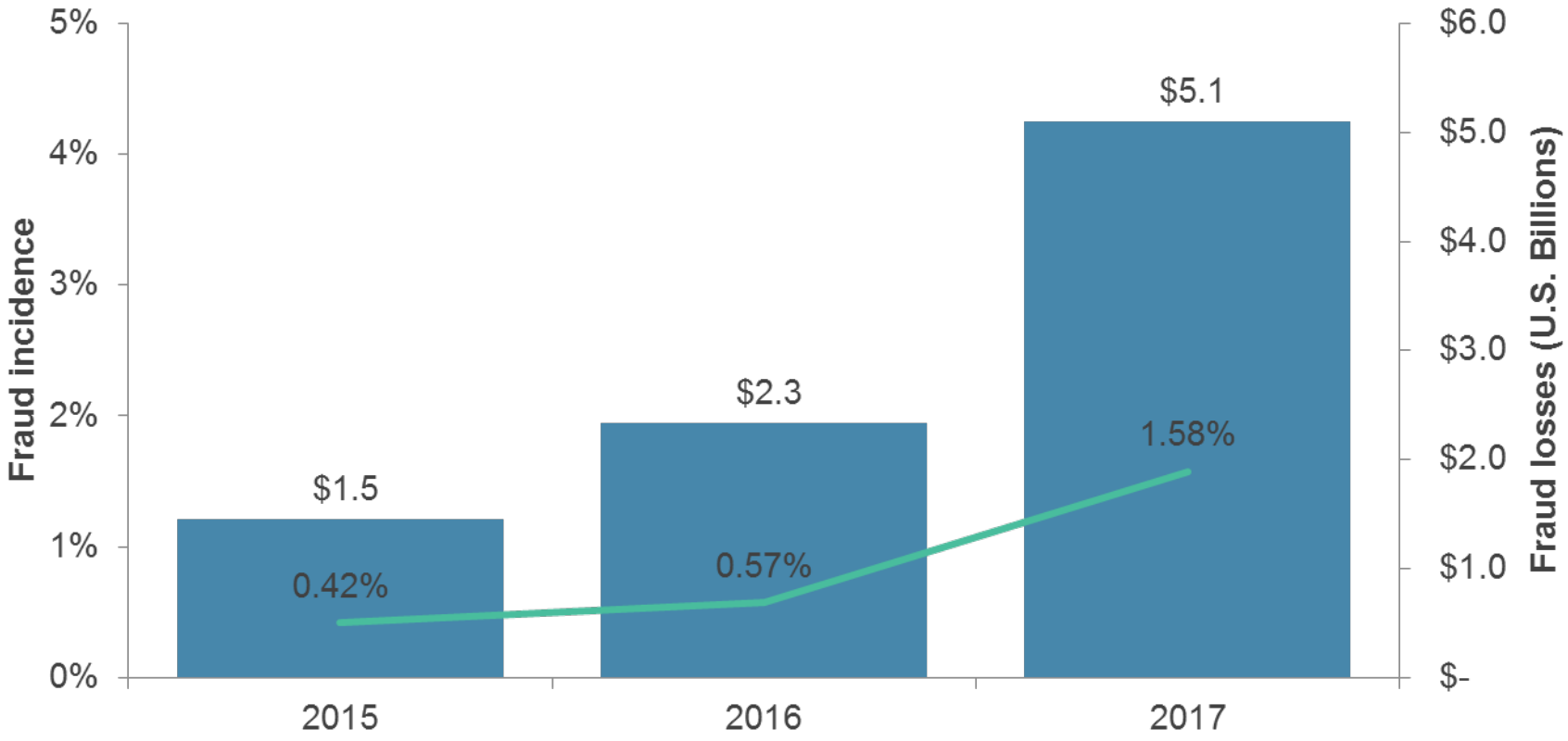
Fraud incidence by breach notification status, 2015-2017



Source: Javelin Strategy & Research, 2018

Account Takeovers Incidence and Losses Have More Than Tripled in the Past Three Years

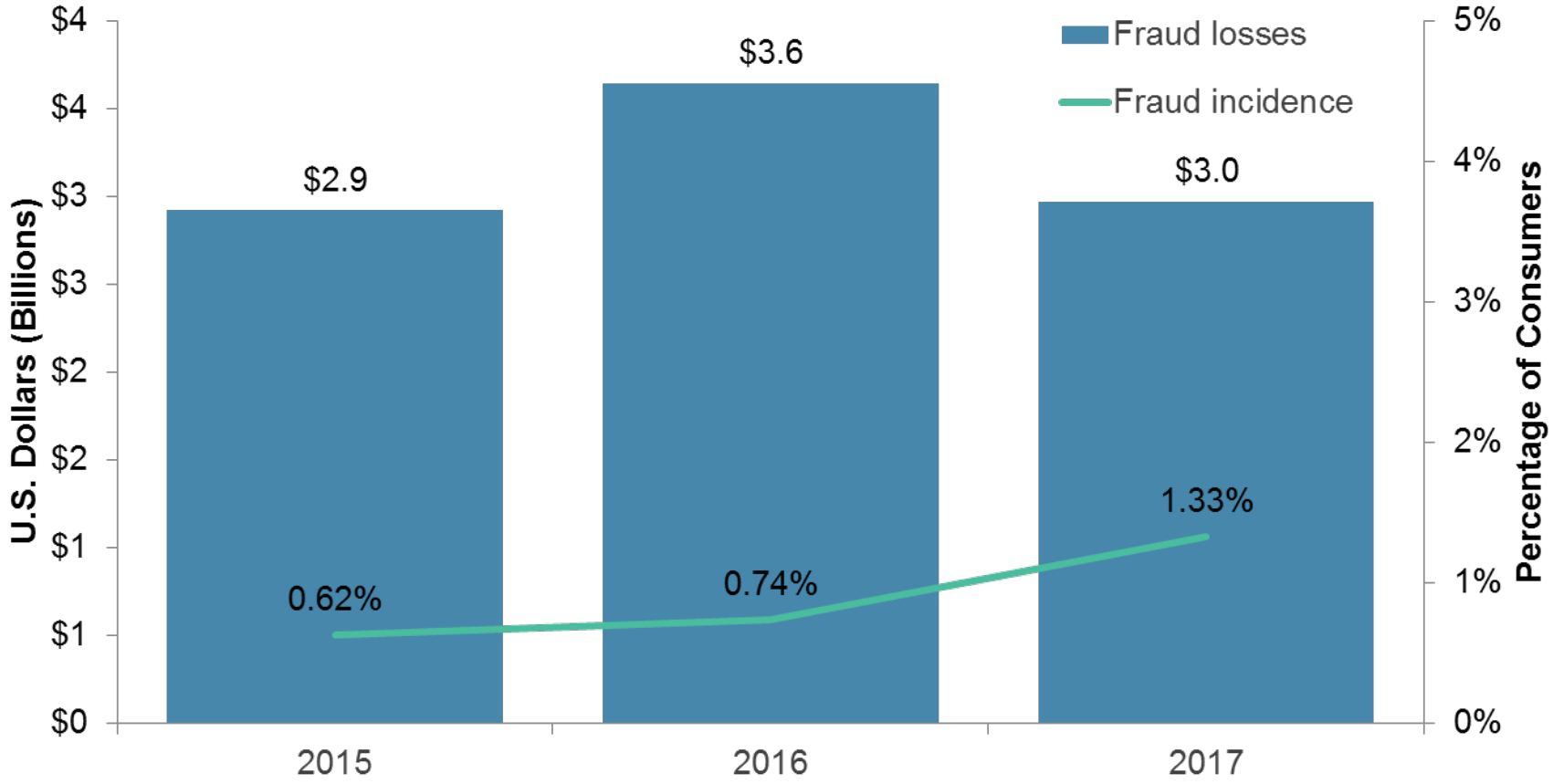
Account takeover incidence and losses, 2015-2017



Source: Javelin Strategy & Research, 2018

A High in New Account Fraud Victims Isn't Accompanied by A Similar Rise in Losses

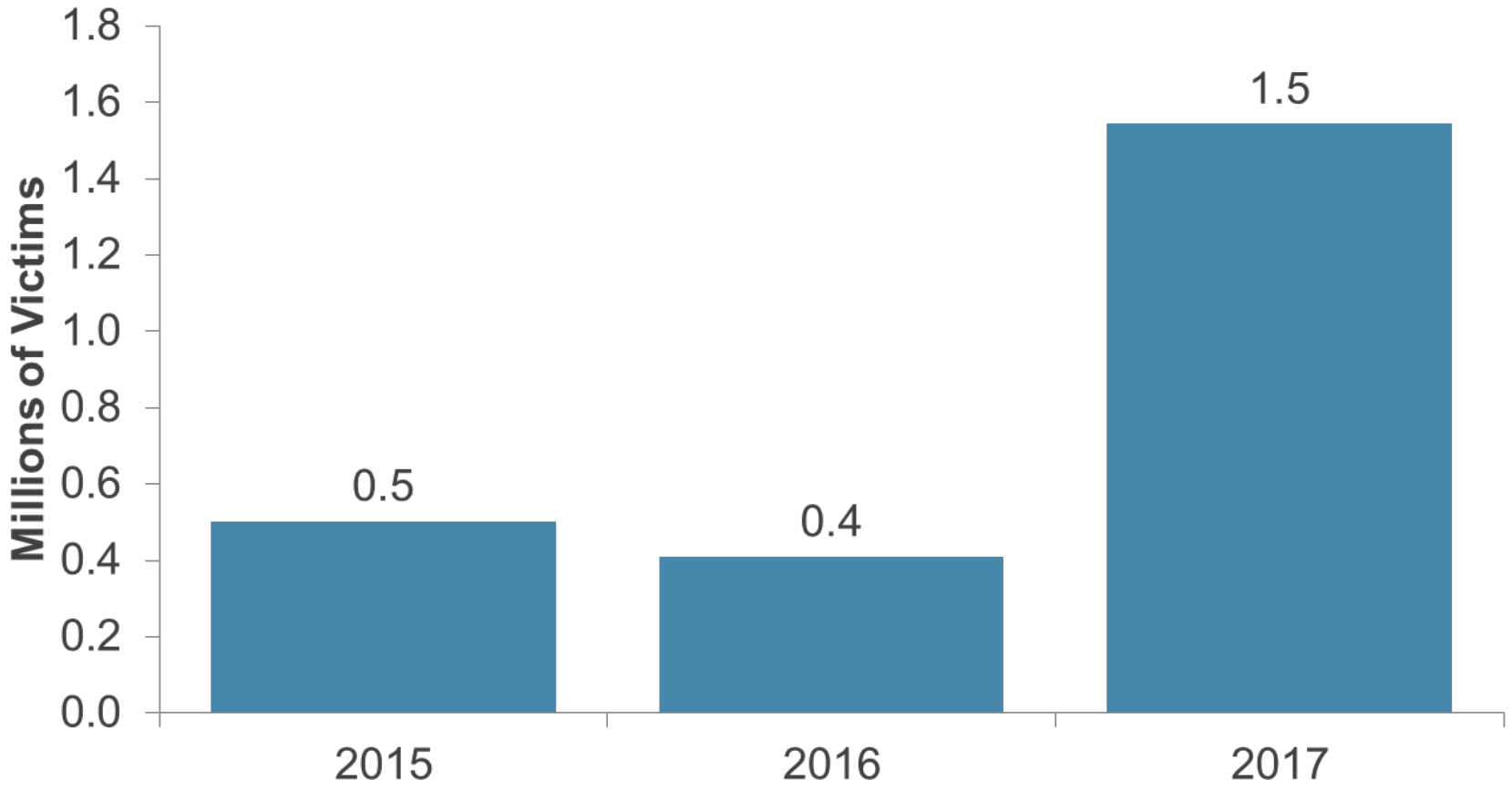
New Account Fraud Incidence and Losses, 2015-2017



Source: Javelin Strategy & Research, 2018

EAF Victims are Experiencing More Complete Impersonation as Fraudsters Close the Loop

Millions of EAF victims with fraudulent intermediary accounts opened, 2015-2017



Source: Javelin Strategy & Research, 2018

Thank You

Al Pascual
SVP, Research
Head of Fraud & Security
al.pascual@javelinstrategy.com

Presentations on Data Breaches

Panel Discussion:

Marc Spitler, Sebastien Gay, Al Pascual

Moderators:

Jared Ho, Marc Luppino

Lunch Break
11:45 am-1:00 pm

Incentives to Invest in Data Security

Panel Discussion:

Lawrence A. Gordon, Matthew P. McCabe, Tyler Moore, Sasha Romanosky, Matthew Sharp

Moderators:

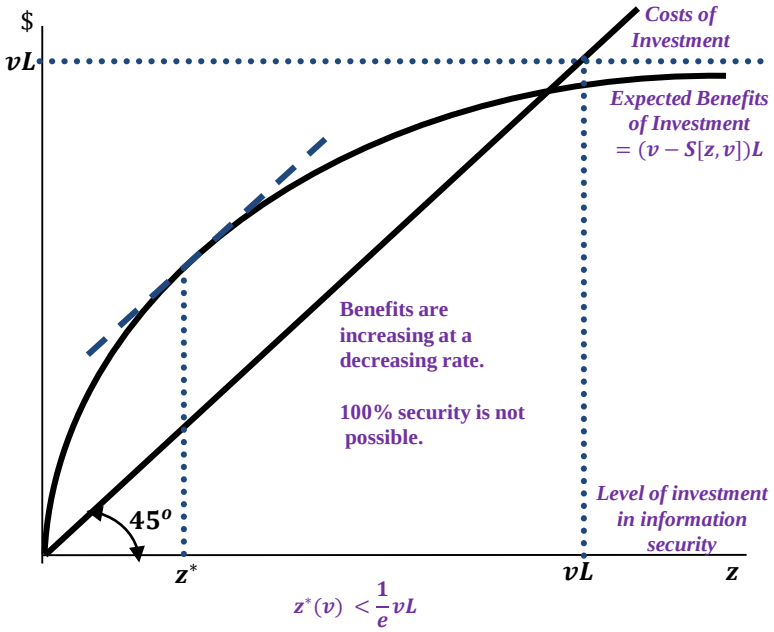
Elisa Jillson, Mike LeGower

Incentives

Customer Trust	Reputation
Ex Ante Compliance	*Ex Post* Liability
Customer Demand	Competitive Advantage
Cost Reduction	Cyber Insurance Coverage

Gordon-Loeb Model for Cybersecurity Investments*

Benefits and Costs of an Investment in Cyber/Information Security*



v – *Vulnerability (Probability of security breach)*
L – *Potential Loss*
vL – *Expected Loss*
z – *Level of Investment*
z^* – *Optimal Investment Level*
$S[z, v]$ – *Revised v after z (Revised probability of breach)*

Optimal Investment Example**

Vulnerability/Threat		Value of Information Sets (in $ Million)				
		Low	Medium			High
		20	40	60	80	100
Low	20%	<2M	<3M	3M	<4M	4M
Medium	40%	<3M	<3M	<4M	<4M	<4M
	60%	<3M	<4M	<4M	>4M	>4M
High	80%	<3M	<3M	<4M	<4M	<4M

YouTube Video explaining the Gordon-Loeb Model:
https://www.youtube.com/watch?v=cd8dT0FuqQ4

BBB Recommends the Gordon Loeb Model

2017 U.S. Better Business Bureau (BBB) report recommends the Gordon-Loeb Model as "...a useful guide for organizations trying to find the right level of cybersecurity investment."

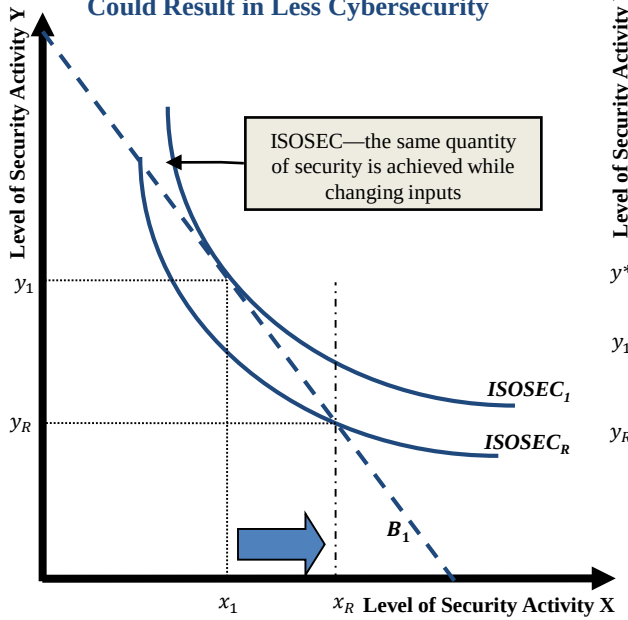
***Gordon, L.A. and M.P. Loeb, "The Economics of Information Security Investment,"** *ACM Transactions on Information and System Security*, November 2002.
****Gordon, L.A., M.P. Loeb, and L. Zhou,** "Investing in Cybersecurity: Insights from the Gordon-Loeb Model," *Journal of Information Security*, March 2016.

Incentives to Increase Cybersecurity Investments in Private Sector Firms*

Why Are Cybersecurity Investments So Difficult to Justify in Private Sector Firms?

- They are primarily cost savings projects rather than revenue generating projects (and savings can't be observed)
- Costs of breaches are largely implicit (reputation & liability) vs. Explicit costs (detecting & correcting breaches)
- Most breaches impact earnings and stock prices in the short-run, but not long-run (customers & stockholders have become tolerant of breaches)
- The risk (uncertainty) of breaches can't be measured precisely & investments are largely irreversible. Wait & see approach may be rational (deferment option)
- Externalities are important, but hard to justify

Government Regulations/Incentives Could Result in Less Cybersecurity



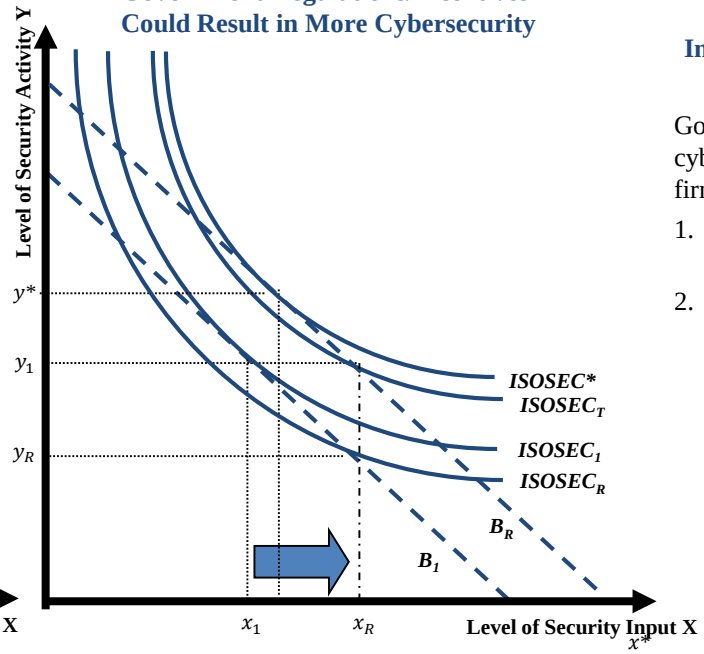
Regulation forcing security input x_1 to increase to x_R results in a decrease in the level of security, if total level of spending (i.e., security budget, B_1) remains fixed and the firm was utilizing the optimal mix of inputs prior to the regulation.

Pre-regulation Security Level 1,
Security Budget: $B_1 = PXx_1 + P_Y y_1$

Post-regulation Security Level R,
Security Budget: $B_R = PXxR + PYyR$

$B_R = B_1$

Government Regulations/Incentives Could Result in More Cybersecurity



Regulation forcing security input x_1 to increase to x_R results in an increase in the level of security, if total level of security spending increases from B_1 to B_R, providing Y inputs are not reduced. The mix of inputs may not be optimal, as shown below ($B_R = PXxR + PYyR$). However, the mix could be optimal, as shown above ($B_R = PXx* + PYy*$).

Insights and Results from Gordon, Loeb, Lucyshyn & Zhou Research

Government incentives/regulations affect cybersecurity investments in private sector firms depending on:

1. Firm's cybersecurity budget is fixed or increases
2. Firm is utilizing the optimal mix of inputs

   Fixed budget/opt mix -- incent/reg: security ↓

   Fixed budget/non-opt mix-- incent/reg: security ↑↓

   Increased budget -- incent/reg: security ↑

***Gordon, L.A., M.P. Loeb, W. Lucyshyn, and L. Zhou, "**Increasing Cybersecurity Investments in Private Sector *Firms," Journal of Cybersecurity*, Vol. 1, No. 1., 2015.
In 2016, NSA awarded this paper Honorable Mention for its contribution to the scientific cybersecurity literature.

Who provides (or should provide) incentives to invest in data security?

A. Culture – security professionals, executives, boards

B. Customers / consumers

C. Cyber insurance

D. Law – state statutes, data breach litigation, federal agencies, etc.

E. Other

Incentives to Invest in Data Security

Panel Discussion:

Lawrence A. Gordon, Matthew P. McCabe, Tyler Moore, Sasha Romanosky, Matthew Sharp

Moderators:

Elisa Jillson, Mike LeGower

Break
2:30-2:45 pm

Consumer Demand for Data Security

Panel Discussion:

Justin Brookman, Michael Higgins, Wiley Hodges, Kirsten Martin, Rick Wash

Moderators:

Jared Ho, Marc Luppino

Consumer Reports by the numbers

7m+
Subscribers

$250m
revenue

1m+
Survey responses

60 state-of-the-art labs

327 acres
at Auto Test Center

7000+
products tested annually

The Digital Standard

Test Name	Criteria	Indicators	Procedure Overview
Functionality Over Time	The company will continue to maintain the intended functionality of the product over the product's expected life cycle.	Every feature of the product will continue to work for as long as I can reasonably expect; that is, the manufacturer will not 'brick' certain parts of the product	
Terms of Service and Privacy Policy documents	I can easily find, read, and understand the privacy policy and/or terms of service.	The Terms of service (ToS) are easy to find. The ToS are available in the language(s) most commonly	Investigation and analysis of publicly available documentation to determine what the company clearly discloses
Data control	I can see and control everything the company knows about me.	Users can control the collection of their information. Users can delete their	Investigation and analysis of publicly available documentation to determine what the company clearly

Key security elements evaluated

Use of encryption	Commitment to support period
Resistance to attacks	Password rules
Vulnerability disclosure program	Security oversight
Automatic/push updates	Multifactor authentication
Best build practices	Reliance on 3P content or libraries
Out-of-band notice of changes	Updates authenticated

Goals

- More information to marketplace
- Empower consumers to make security-conscious choices
- Provide accountability for poor security practices
- Push companies toward stronger security

Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds

Glow has responded by fixing the problems and updating the app

By Jerry Beilinson
July 28, 2016

Glow is a mobile app designed to help women track their menstrual cycles and fertility. Like similar apps, it asks users to record the onset of their periods, along with details such as their weight and medications. Glow also asks for intimate physical details, including the appearance of their cervical mucous and the position of their cervix (the app has instructions for determining these characteristics), any history of abortions, whether they've experienced anything from diarrhea to low sex drive, their mood, and more.

Recently, Consumer Reports tested Glow for security and privacy features as part of a broader project, and found surprising vulnerabilities. One security flaw might have let someone with no hacking skills at all access a woman's personal data. Other vulnerabilities would have allowed an attacker with rudimentary software tools to collect email addresses, change passwords, and access personal information from participants in Glow's community forums, where people discuss their sex lives and health concerns.

15

Mobile security software in Our Ratings.
Current Mobile security software Ratings

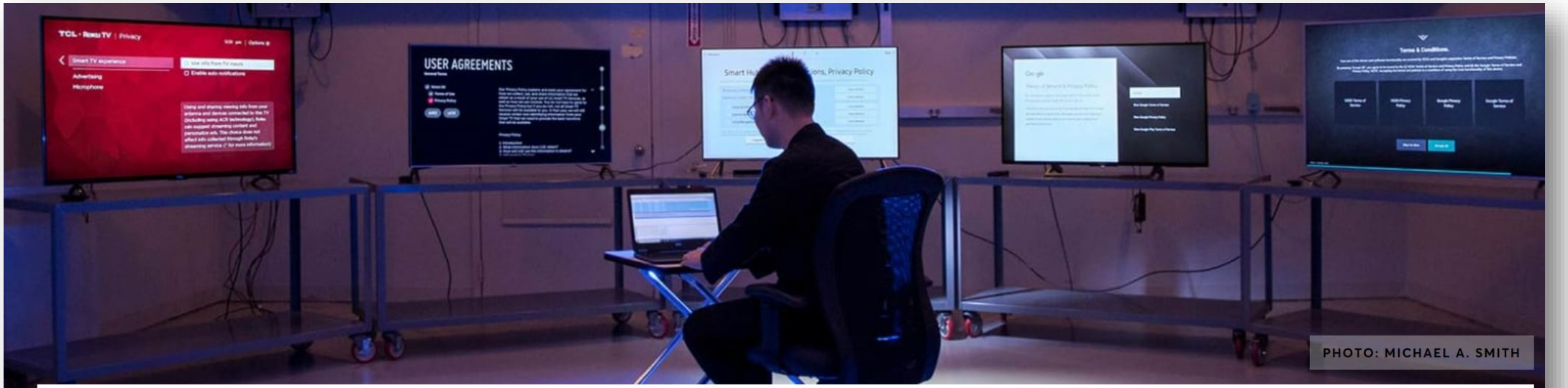


PHOTO: MICHAEL A. SMITH

Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.

WORSE — BETTER

MOBILE PEER-TO-PEER PAYMENT SERVICES

SERVICE	OVERALL SCORE	PAYMENT AUTHENTICATION	DATA SECURITY	DATA PRIVACY	CUSTOMER SUPPORT	BROAD ACCESS
Apple Pay	76	⏫	⬆	⏫	⬆	➖
Venmo	69	⬆	➖	⬇	⏫	⏫
Cash App (Square)	64	➖	⬆	⬇	⬆	⏫
Facebook P2P Payments in Messenger	63	⬆	⬆	⬇	⬇	⏫
Zelle (standalone app)	50	➖	⬇	⬇	⏫	➖

Security testing challenges

- Public documentation often lacking
- Lack of initial visibility into update frequency and quality
- Black box/server-side difficult/impossible to test
- Difficult to adapt and scale suite of tests to broad range of consumer products
- Score subjectivity
- How assess patched vulnerabilities
- Practices can change with little discoverability

Limitations on demand-driven approach

- Externalities not felt by consumers
- Difficulty in assessing security risks
- Testing provides imperfect information
- Attribution difficult and delayed
- Need for legal baseline security requirements

How important is perceived security to consumers making purchasing decisions?

A. Important, but they expect the firm to be responsible for security.

B. Important, and they understand that security is a shared responsibility between themselves and the firm.

C. Moderately important, and they expect firms to be responsible for security

D. Moderately important, and they understand it's a shared responsibility.

E. Not important, because consumers don't expect security.

F. Other

Trade-offs

Cost
Productivity
Usability
Functionality
Latency
Other

Consumer Demand for Data Security

Panel Discussion:

Justin Brookman, Michael Higgins, Wiley Hodges, Kirsten Martin, Rick Wash

Moderators:

Jared Ho, Marc Luppino

Closing Remarks

Jim Trilling

Federal Trade Commission

Division of Privacy and Identity Protection

Thank You,

Join Us Tomorrow