



Supporting the Aftermath of a Major Cyber Security Incident

10.28.15

Ken Skinner
Vice President
Customer Support

The Identity Theft Landscape

#1

CONSUMER COMPLAINT

Identity theft was the top FTC consumer complaint for the 15th consecutive year

12.7M

INDIVIDUALS

The number of consumers affected by identity fraud in 2014

\$16B

TOTAL COST

The total cost of identity fraud for consumers in 2014

Sources: Javelin Strategy & Research, FTC

That's Where We Come In



CSID is a leading provider of global enterprise level identity protection, and fraud detection solutions and technologies.

- ✓ Reporting and monitoring of credit data
- ✓ Reporting and monitoring of personal information
- ✓ CyberAgent® - Dark web monitoring
 - Stolen personal data
 - Malware
 - Potential threats
- ✓ Personal identity theft restoration
- ✓ Customer Care



Our Turnkey Platform Powers More than 80% of the Identity Protection Market

The screenshot shows the CSID Internet Monitoring dashboard. At the top, there are navigation tabs for Home, Internet Monitoring, Identity Theft Protection, Lost Wallet, and Education Center. The main content area is titled "Internet Monitoring" and includes a section for "SELECTED MONITORING RECENT ACTIVITY". Below this, there is a table of activity logs with columns for Type, Date, and Title. A prominent warning box states: "Your CreditCard Card was compromised online. It is possible that this information has been wire-tapped, or hacked for illicit purposes, including identity theft." Below the warning, there is a table of "Additional Data" for a compromised credit card, listing details such as First Name, Last Name, Street, Phone Number, Credit Card Number, Credit Card Exp. Date, Credit Card CVN, and Service Date. At the bottom, there are instructions titled "Here's What You Can Do" with three numbered steps.

The screenshot shows the myFICO Monitored Data dashboard. It features a progress bar indicating "55% Complete" for monitoring data. A green checkmark icon is visible next to the progress bar. The main content area is titled "Monitored Data" and includes a section for "PERSONAL INFORMATION" with details for Bryan HjelM, including a date of birth and a phone number. To the right, there is a list of "Common Tasks" such as "Receive Text Alerts", "Update Account Information", "Update Billing Information", "Add a Member", "View Account History", "Change User ID", and "Change Password".

The screenshot shows the LifeLock Alerts and Reports dashboard. At the top, there are navigation tabs for HOME, ALERTS AND REPORTS, MANAGE ACCOUNT, and SUPPORT. The main content area is titled "Complete Your Profile" and includes a progress bar for "55% profile completeness". Below this, there is a "Message Center" table with columns for Date, Description, and Status. A "Monthly Credit Score" section shows a score of 779 for Feb 23, 2015, with a trend line and a score of 815 for Jan 28, 2015. There is also a "LifeLock Alert Network - Identity Alerts" section with a bar chart showing the number of alerts sent for different months. The chart shows a significant increase in alerts for March 2015, with 9,477,533 alerts sent, compared to 923,562 in February 2015.

Vulnerability Through Third Party Vendors



TARGET – Nov. 2013

70M phone numbers and emails
40M payment card records

- ❑ A contractor with a presence in Target's data center was breached
- ❑ Perpetrators used contractor's system credentials to gain access to Target's POS systems
- ❑ Uploaded malware (BlackPOS) collected Type I & II data
 - unencrypted customer PII and payment card information stolen
- ❑ Over 11GB of data from 1797 Target stores breached

Vulnerability Through Employee Error



The White House – April 2015

Gained access to President's private schedule and some email correspondence

- ❑ State Department employee opened a malicious link in an email
- ❑ Hackers used that access to conduct another phishing attack in part of the White House network
- ❑ Breach discovered in the unclassified network that served the Executive Office of the President

Vulnerability Through Espionage



OPM – June/July 2015

25M+ government employees, retirees, and contractors impacted

- ❑ **June 2015:** Office of Personnel Management (OPM) announces cybersecurity incident compromising personnel records for 4.2 million current and retired personnel - **(OPM1)**

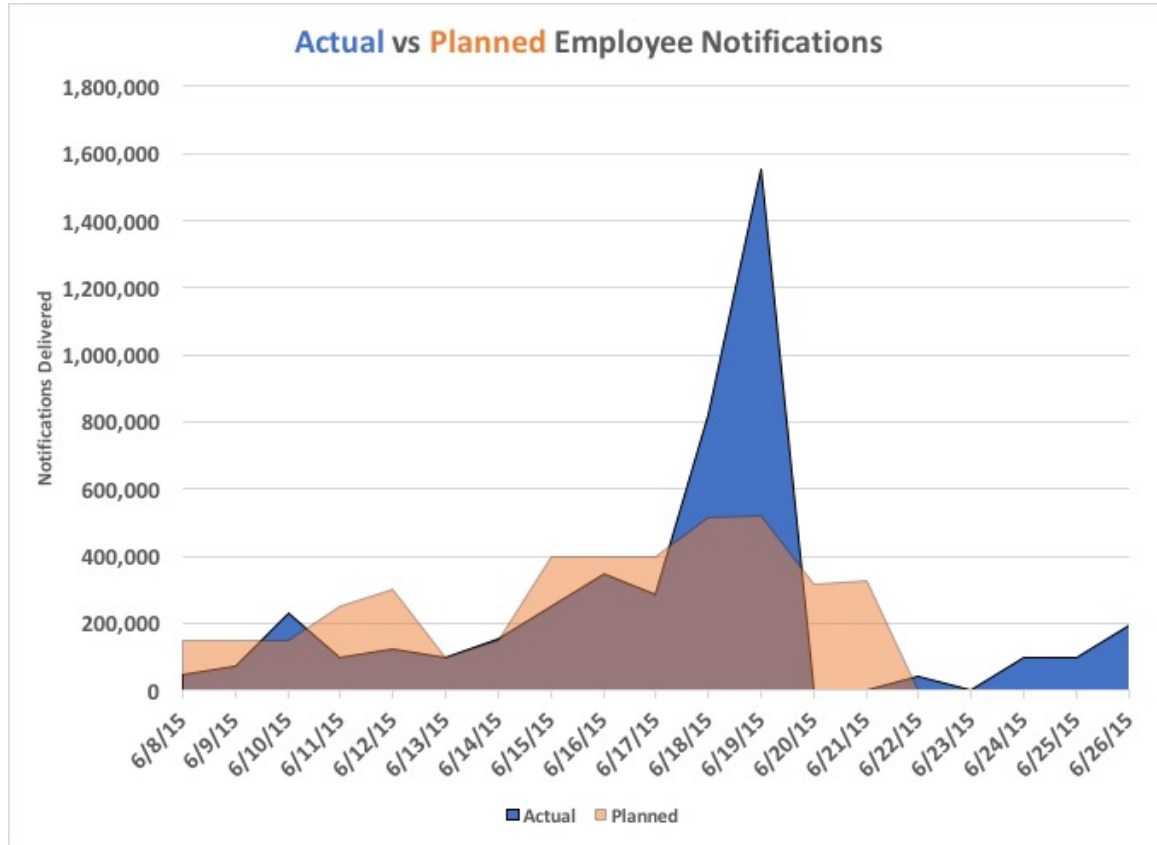
- ❑ **July 2015:** OPM announces cybersecurity incident compromising background investigation data for 21.5 million employees and contractors - **(OPM2)**
 - SF 85, SF 86 forms in place since 2000
 - 19.7 million applicants and 1.8 million SO
 - 5.6 million finger prints

OPM1 Contract Award

- Winvale/CSID notified of award on June 2
- Portal, Notifications Delivery, and Call Centers to be operational on June 8

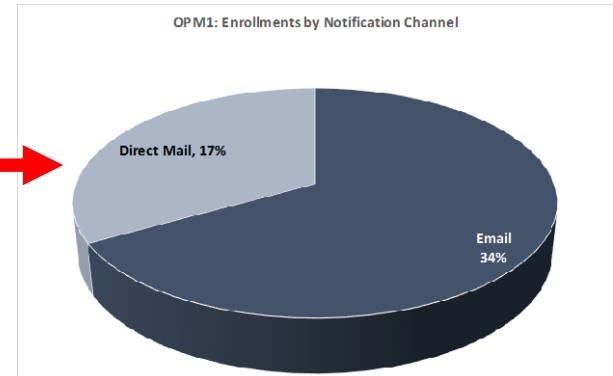
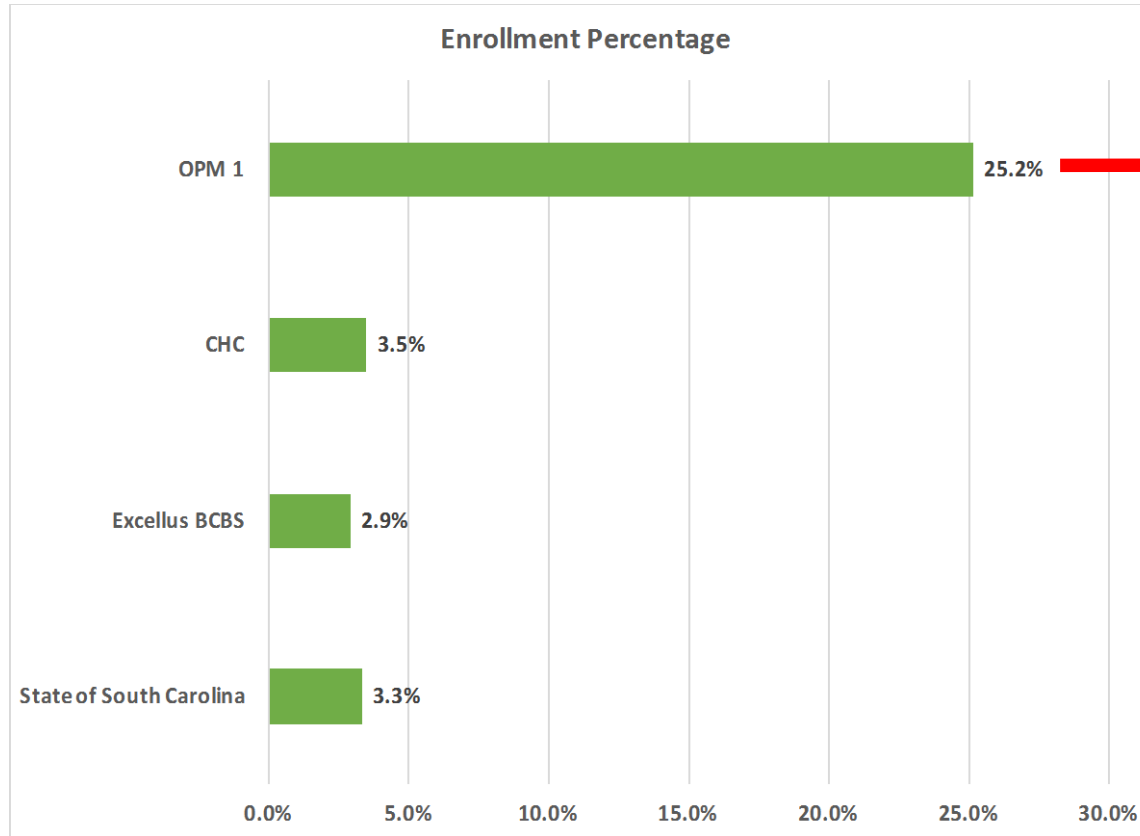


OPM1: Timing and Outcome of Employee Notifications



- **June 8:** notifications began
 - 2.17 million direct mail
 - 1.98 million email
 - June 21 completion
- **June 8-17:** 69% of **planned** notifications delivered
 - Emails halted from June 11 - 13
- **June 18 & 19:** 57% of **total** notifications delivered

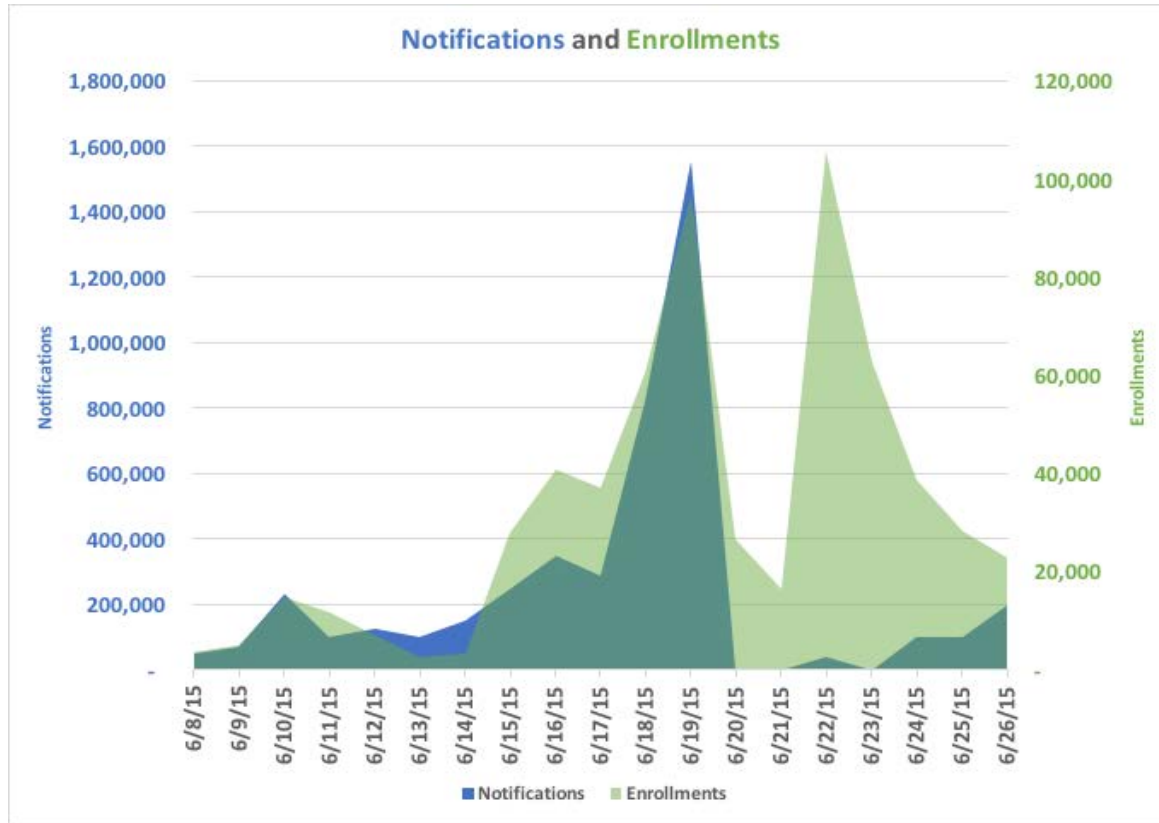
Breach Enrollments as a Percentage of Notifications



Why?

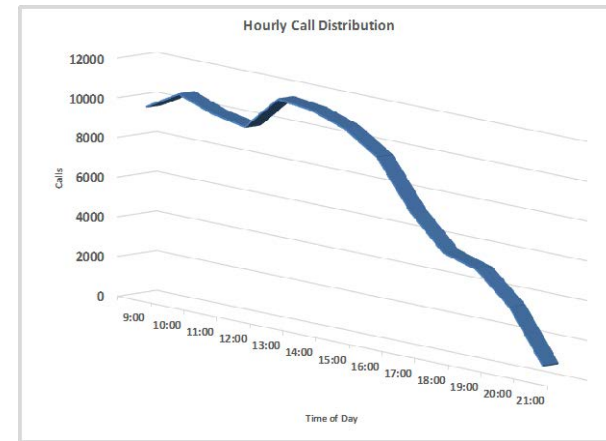
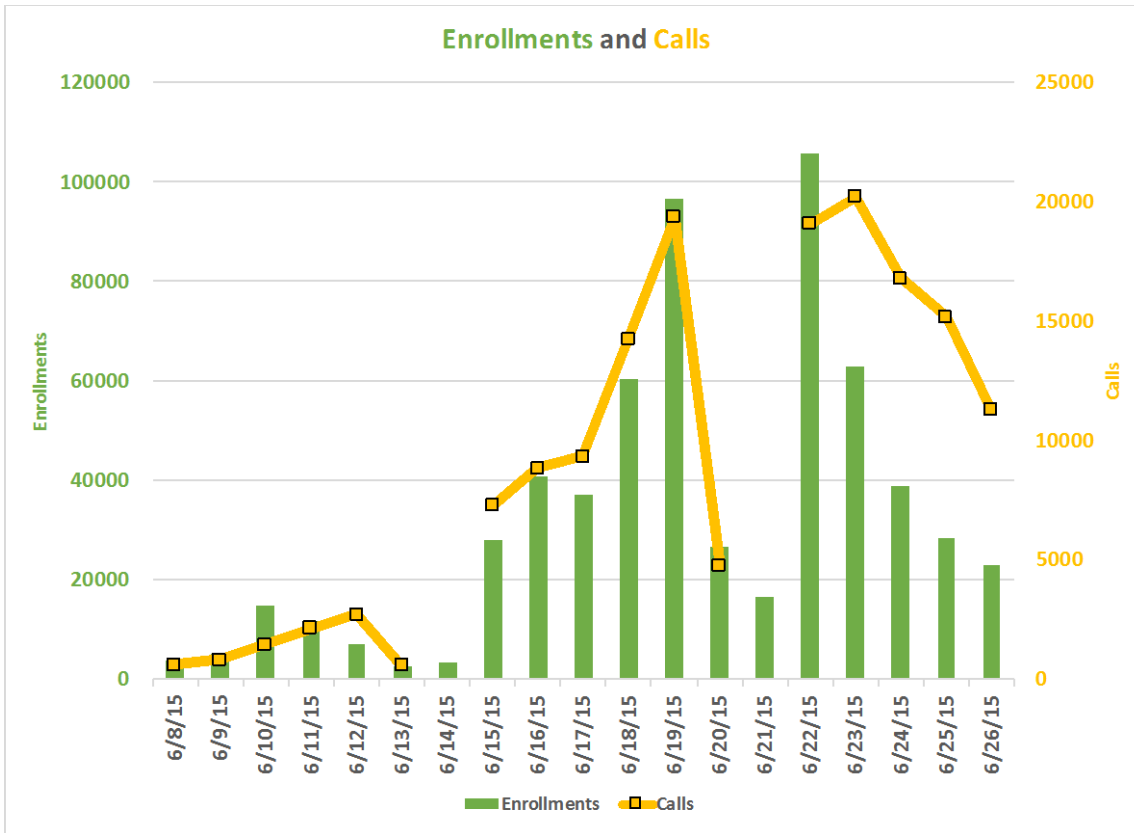
1. Type of breach
2. Employer/Union involvement
3. Email sent to agency domain
4. Media

OPM1: Timing of Notifications and Enrollments



- **Factor 1:** short notification period
- **Factor 2:** high enrollments to notifications ratio
- **Factor 3:** notification plan not executed
 - email notifications plan changed the most and had the most impact
 - Notifications delivery shortened from 14 days to 12

OPM1: Timing of Enrollments and Call Center Activity



- Forecasted 5000 calls per day over 1st three weeks
 - 10% take rate
 - 25% calls to enrollments
- Actual average calls per day over 9000
 - **Factor 4:** Informational calls routed to enrollment number

OPM1 vs OPM2

OPM1	OPM2
Largest employee breach – 4.2M affected	Largest employee/contractor breach – 21.5M
Highest known breach percentage enrollment 25% - over 1.1 million	?
5 days from award to live	1) 6 weeks requirements definition prior to release of BRD 2) 2 months from award to live
12 day notification period for affected	60 day notification period for affected
Email and Direct Mail notification	Direct Mail notification only

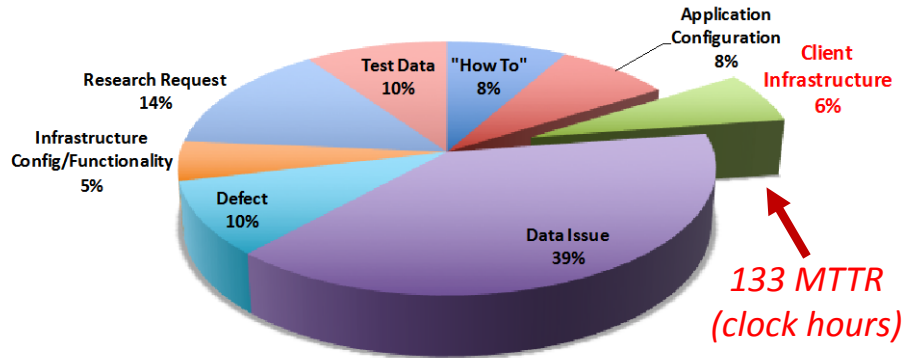
A Vendor Perspective: SaaS/PaaS vs. On-Premise Software

- CSID is a B2B2C company (exception - some breaches)
- Business environment has a high cost
 - connecting to data sources
 - governmental and commercial data access and security certifications
- SaaS/PaaS allows a focus on functionality rather than infrastructure

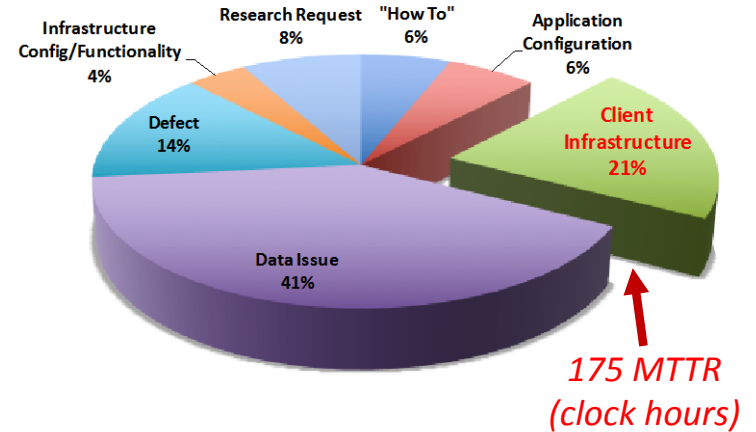
Benefit	Outcome
Faster delivery of features	User productivity/revenue
Real time application monitoring	Continuous service improvement
Real time remediation & scalability	Application availability and performance
More control over application delivery	More responsibility: support, business continuity

A Support Example: SaaS vs. On Premise

SaaS Clients



On-Premise Client



Client Infrastructure incidents are the 2nd highest MTTR of any incident type

Closing Thoughts



- Follow IT rules and regulations.
- Carefully consider the impact of changes to project deployment plans.



Use data!

- Cost and incidence of identity theft are increasing.
- Identity restoration is costly and highly impactful.





Ken Skinner

*Vice President,
Customer Support*

QUESTIONS?

kskinner@csid.com

www.csid.com

What Are the Affected Receiving?

	OPM1	OPM2
Credit Monitoring	3 bureau	3 bureau
Credit Reporting	1 bureau	3 bureau
Non-credit Monitoring	Change of Address/Court Records/Sex Offender/SSN Trace/Non Credit Loan	Change of Address/Court Records/Bookings/Sex Offender/SSN Trace/Non Credit Loan
Cyber Monitoring	yes	yes
Identity Theft Insurance	\$1mm	\$1mm
Early Warning System	no	Bank Account
Full Service Restoration	yes	yes
Child Coverage	no	Cyber/SSN Trace
Coverage Expires	12/8/2016	12/31/2018