OFFSHORING AMERICAN CALL CENTERS:
The Threat to Consumers, Communities, and National Security
EXECUTIVE SUMMARY

In recent years, U.S. companies exported more than 500,000 call center jobs to India, the Philippines, Egypt, Mexico, Honduras, and other developing nations. Call centers are a valuable source of jobs in the United States, employing as many as five million Americans—nearly four percent of the U.S. workforce. Recent technological advances have made it easier to transfer these jobs overseas to lower-paid, less regulated workers, a trend that increases risks for consumers and devastates communities nationwide.

The offshoring trend has evolved into a crisis for consumers, with fraud and identity theft becoming a multi-million-dollar business. For example, in one widely reported scam, criminals used foreign call center workers to make 2.7 million calls and collect some $5.2 million through threats and intimidation, alleging that innocent consumers owed money for past loans.

In the current economic landscape, with millions unemployed and the recovery shaky, U.S. workers and the communities in which they live need these call center jobs. In response, the U.S. Congress is taking action. Both the House of Representatives and the Senate are reviewing bills to keep call centers in the United States and to end federal rewards and incentives for offshoring. At least seven state legislatures are moving forward on similar legislation.

The Consequences of Offshoring

Federal action is essential because the consequences of offshoring are destructive on many levels, devastating individuals, communities and the nation.

- Consumers’ financial and medical data become vulnerable to theft and misuse by poorly regulated contractors overseas.
- Communities that subsidized call center expansion a few years ago are devastated by the sudden loss of jobs and revenue.
- Laid-off workers and their families join the rolls of the unemployed and often lose their sense of independence along with their paychecks.
- National security may be threatened as more financial, medical, and personal data about American corporations and citizens falls into the hands of contractors in less stable nations.

Despite such clear vulnerability to fraud, four large banks — Bank of America, J.P. Morgan Chase, Wells Fargo, and Citigroup — have recently moved call center operations to the Philippines, a country that lacks even the most basic safeguards for security, privacy, and legal accountability.

In addition to the threat to consumers’ wallets, offshoring presents a threat to civil liberties. Once data is moved overseas, Fourth Amendment protections from warrantless searches disappear.

Finally, given the instability of some new offshoring sites, data security must be given even more serious scrutiny. Egypt, which recently experienced an unexpected political upheaval during the “Arab Spring,” is rapidly becoming one of the most popular locations for new call centers.

Bi-partisan Support from Congress and the Public

Legislation now pending in both the House and Senate addresses the multiple threats posed by increased offshoring of call centers. Both the House bill (H.R. 3596) and the Senate bill (S.3402) are designed to keep jobs in the United States and improve protections and service for consumers.
**U.S. CALL CENTER WORKER AND CONSUMER PROTECTION ACT — H.R. 3596 AND S. 3402**

This bi-partisan legislation would:
- Require call center agents to reveal their locations to U.S. consumers and transfer customers to U.S. call centers upon request.
- Prohibit companies that move call center jobs overseas from receiving federal grants and loans.
- Give preference on government contracts to companies that keep call center jobs at home.

Voters across the political spectrum support legislation to keep call centers at home. An August 2012 survey of likely voters nationwide found that the vast majority strongly support proposals to limit the offshoring of call center jobs. According to the survey, 90 percent support proposals that would give customers the right to request transfer to a U.S.-based customer service agent. An overwhelming number of respondents support prohibitions against giving federal loans (81 percent) and grants (75 percent) to companies that send call center jobs overseas. Three-quarters (78 percent) rated overseas call centers negatively, including 79 percent of Democrats, 75 percent of Republicans, and 78 percent of Independents.

**BREAKING DOWN THE CALL CENTER THREAT**

If you think about the scenario, you have the lowest-paid contractors furthest away from the main office, all with access to sensitive data. It’s an incredibly risky proposition.
—Paul Bilden, Covelight Internet security company

Many U.S. companies are taking advantage of cheaper labor costs by relocating facilities to the developing world. India is the most well-known magnet for call centers, but last year the Philippines surpassed India with some 400,000 workers devoted to answering Americans’ calls. Companies also are moving quickly into China, Saudi Arabia, Egypt, Mexico, and the Czech Republic, among other sites. The result for consumers:
- Lack of security for private records—including financial and medical records.
- Loss of millions of dollars to fraud.
- Violation of Fourth Amendment protections against warrantless search and seizure.

**Hundreds of Thousands of Security Breaches**

Threats to consumers’ private data are not new. For at least a decade, security breaches in overseas call centers have been reported in the U.S. and European press. Foreign call center workers have peddled customers’ financial and health information to criminals, defrauded consumers of millions of dollars by posing as debt collectors, and stolen hundreds of thousands of dollars from bank customers.

The U.S. Federal Trade Commission has been investigating scams defrauding Americans. For example, Citibank customers in the United States lost more than $400,000 to Indian call center scams. British bank customers have also lost hundreds of thousands of pounds, and journalists have gained access to private bank account records.

In 2012 a call center ring based in India scammed consumers by impersonating workers from Microsoft and Apple, gaining access to personal information by offering to do security checks. In the Philippines and India, call center employees have been arrested for a variety of schemes to steal consumer financial data and make off with thousands of dollars from American Citibank and HSBC.
Although India is more advanced than most other developing nations in terms of technology and security, it has yet to be approved by the EU as a “data safe” nation. European companies are increasingly wary of transferring critical business information to Indian contractors, with good reason. The New York State Department of Labor has expressed similar concerns about data security abroad, particularly for the medical and financial industries.

Although private companies and the Indian government downplay security risks for obvious reasons, independent security analysts find that “costs are being cut somewhere and many a time it is security.”

“We know this business is out of control,” police sources told UK journalists earlier this year. “The simple fact is the banks are worried that their customers will get scared and swap banks if they learn how easily and cheaply their confidential details are sold.”

Although India has taken steps to improve its data privacy laws, the government specifically omitted outsourcing companies from such regulations in 2011. The Times of India reported that the government caved in to pressure from the multi-billion-dollar outsourcing industry.


Companies are understandably reluctant to report security breaches, fearing negative publicity. But one study of the problem completed in 2005 found that 83 percent of Indian outsourcing companies had experienced information security breaches.12

Overseas call centers have not only defrauded companies and stolen from consumers, they’ve also used health records as blackmail tools against management, stolen valuable data from tech company databases, and attempted to sell trade secrets from American software companies to Indian competitors.13

The Indian government is not taking measures to address the problem. The Indian parliament passed a new data privacy law in 2011, but outsourcing companies were specifically exempted from the regulations.14

**Lax Laws and Even More Lax Security**

In foreign countries, background checks of employees that measure up to U.S. standards are difficult and expensive, but they are clearly necessary. Up to one-fourth of all call center applicants outside the United States provide false information on applications.15

For the most part, there are no central criminal databases in developing countries, and credit rating agencies are relatively new. Therefore, background checks are most often done in person, a time-consuming and invasive process, costing $30 to $1,000 per employee. In the United States, a more thorough vetting usually costs less than $100 per employee.16

Investigators face several obstacles when seeking information about potential employees, including the lack of permanent ID numbers, such as social security cards, to help track workers. Many police departments in developing nations do not store or organize criminal records carefully.

**More Call Centers, Less Security in the Philippines**

In 2011, the Philippines surpassed India as the main destination for offshore call centers. But the Philippines
has even fewer legal protections to stop data breaches than does India.

More than 400,000 Filipinos work in call centers for companies as diverse as T-Mobile, JP Morgan Chase, and Expedia. There are currently no regulations in the Philippines governing data protection, although a law is under consideration to make the country compliant with Organization for Economic Cooperation and Development (OECD) standards.\(^\text{17}\)

Clearly, the strict security measures followed by U.S. companies are simply absent in many other countries. And once a crime has been committed at an offshore call center, a complex variety of laws and legal systems frequently thwart attempts to identify and prosecute the culprits.

### THE PHILIPPINES

- 400,000 call center workers
- No regulations governing data protection

Warrantless Surveillance: Bypassing the Fourth Amendment

Threats to data security in foreign call centers can come from another—perhaps unexpected—source. As a result of offshoring, U.S. consumers’ personal and financial data is subject to warrantless federal surveillance.

In June 2011, consumers brought a class-action lawsuit against American Express, charging that the company’s customer calls are routed to foreign call centers without the callers’ permission or knowledge. This subjects consumers to intrusive and warrantless investigations by the federal government. A similar lawsuit was brought against Bank of America two months later.\(^\text{18}\)

The root of these breaches of citizens’ fourth Amendment protections is the transfer of financial and other data overseas. Once information is at a foreign call center, and as long as one individual’s data is not specifically targeted, that data legally can be collected and analyzed by U.S. federal agencies without a warrant.

Offshoring Harms American Communities

Call centers have become economic lifelines in many American communities over the past 20 years, as U.S.-based manufacturing jobs have disappeared. Local governments have committed millions in tax dollars to fund incentives to lure companies, only to watch those companies offshore call center jobs a few years later, leaving their citizens unemployed and disillusioned.

This year, T-Mobile closed seven U.S. call centers, putting 3,300 employees out of work—after accepting $61 million in state and local subsidies.\(^\text{19}\) Instead of closing some of its call centers in Honduras or the Philippines, T-Mobile prefers to shutter U.S. workplaces.

Wells Fargo followed a similar route—laying off hundreds and moving operations to the Philippines, while workers in Florida, California, and Pennsylvania were left jobless. The banking giant, which received more than $25 billion in federal TARP money during the darkest days of the recession, is tripling the number of its Filipino employees and has asked some U.S. employees to train their own replacements.\(^\text{20}\)

Sykes, a company that handles support and technical calls, took millions of dollars in loans and tax breaks from small towns in Oregon and Florida, where it located new call centers. Just a few years later it relocated operations to Asia. Town leaders pleaded with the company, citing enormous investments of taxpayer money—but Sykes left anyway, and hundreds of workers lost their jobs.\(^\text{21}\)

A depressed town in a small southwest Virginia county lost 250 desperately-needed jobs when Travelocity shut down a call center and moved to India.\(^\text{22}\)

When a call center closes in a small or medium-size community, the result is a major blow to the economy. Retail businesses are shuttered when paychecks disappear. The devastation of so many communities during the continuing recession is indefensible.
Consumers and National Security

A new trend in offshoring may mean even greater risk for American consumers’ money and sensitive information. Call centers are now locating in a broader variety of developing nations with lower wages—and less stable political regimes.

In the final years of the Mubarak regime, Egypt became a major site for new call centers. Egypt actively sought subcontracting from India, hoping to gain a foothold in the industry with its multilingual workforce.

Today Microsoft, Ericsson, Vodafone, and Alcatel all have call centers in a “smart village” in Egypt. Yet the new regime is still a major unknown and lacks the stability that can ensure the safety and security of sensitive financial and personal data.23

Quality Customer Service

Derrick, a CWA-represented call center employee in Jacksonville, Florida, summed up the pride he takes in a job well done. “What more can you say about a job where you get to hear ‘thank you’ everyday—especially ‘thank you for being an American.’”

As overseas call centers take over customer service functions, U.S. consumers often meet frustration, delays, and roadblocks as they seek information. U.S. call center employees have a better understanding of an American caller’s language and cultural context, and typically are more highly-trained and experienced in answering questions.

U.S. call center employees receive more training and have more experience on the job than overseas call center workers. Two-thirds (62 percent) of Indian call center employees have less than one year job tenure, compared to nine percent at U.S. based union-represented call centers.24

Some employers, recognizing that high quality service improves their bottom line—are bringing offshored work back to the United States. AT&T, for example, transferred 5,000 DSL tech support jobs to American workers, and U.S. Airways returned reservation agents to three U.S. call centers in 2011.25

HOW H.R. 3596 and S. 3402 WILL HELP

Legislation now before both Houses of Congress (S. 3402 and H.R. 3596) takes aim at the problem of offshore call centers—sometimes referred to as modern-day sweatshops—that exploit foreign workers, traffic in identity theft and fraud, and regularly mishandle sensitive personal data.

BI-PARTISAN LEGISLATION FIGHTS OFFSHORE CALL CENTERS

The bills before the U.S. House and Senate now will go a long way toward stopping the flow of jobs overseas and bringing them back to American cities and towns to support middle-class families.■
Endnotes


10 Tom Bristow, “Trading Standards warning over Asian call centres targeting Norfolk homes every day with computer ‘fault’ scam,” EDP 24, February 7, 2012 (http://www.edp24.co.uk/news/crime/trading_standards_warning_over_asian_call_centres_targeting_norfolk_homes_every_day_with_com puter_fault_scam.h)


The Communications Workers of America (CWA) is the union for the Information Age, representing 700,000 workers in communications, media, airlines, manufacturing and public service.

CWA is the Customer Service Union, representing 150,000 customer service workers employed at call centers in telecommunications, airline passenger services, the public sector, and the news media. CWA customer service members help customers with technology support, information requests, billing and service inquiries, and sales assistance.