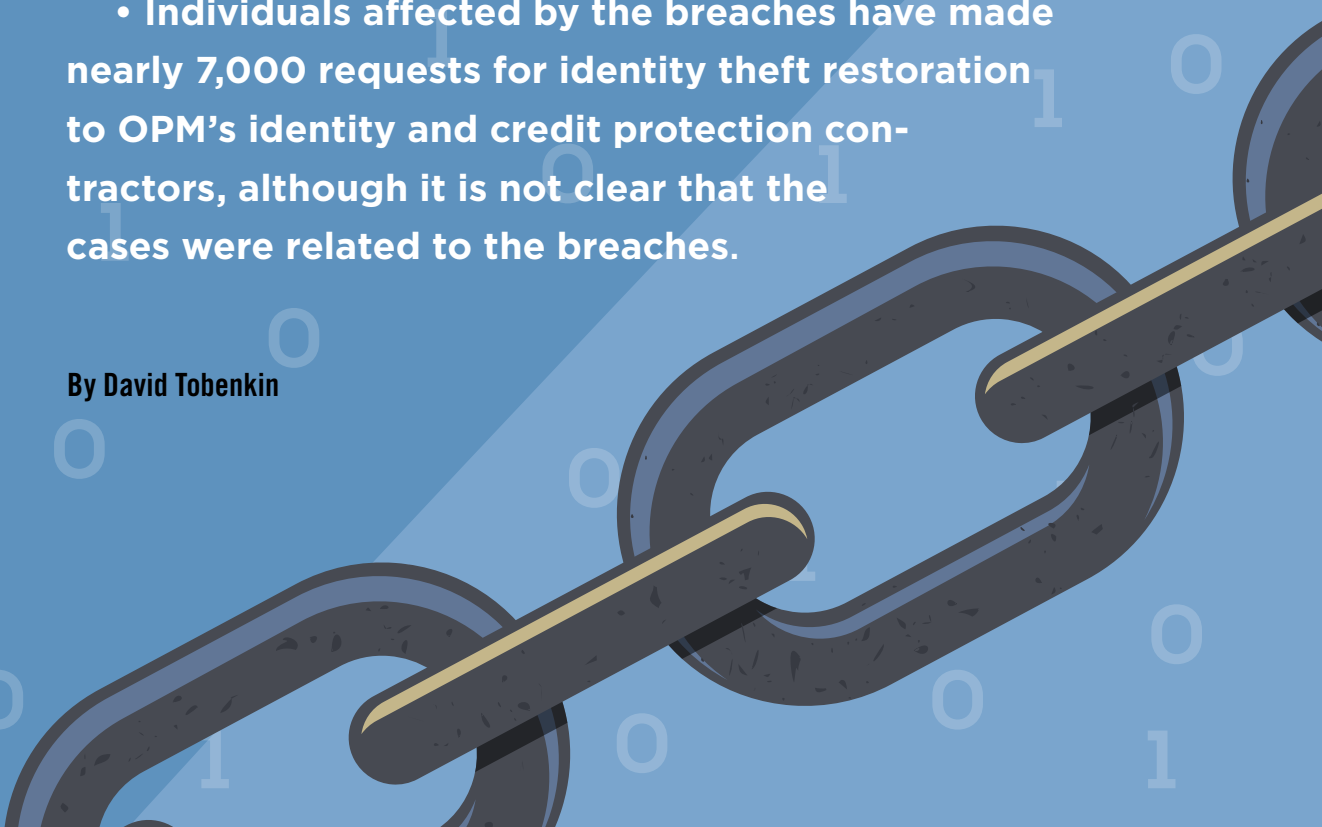


Protecting Identities, Data AFTER THE

NEARLY A YEAR AFTER THE REVELATION BY THE U.S. OFFICE OF PERSONNEL MANAGEMENT (OPM) OF TWO monumental data breaches, the repercussions of the disclosure of the sensitive personal information of more than 22 million federal employees, retirees, contractors and federal job applicants continue to unfold:

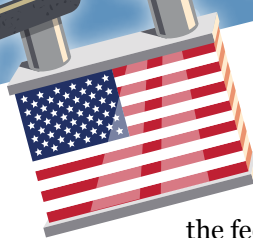
- Congress has extended identity theft protection to those affected from 18 months and three years, depending on the breach, to 10 years; but sign-up thus far has been limited.
- Individuals affected by the breaches have made nearly 7,000 requests for identity theft restoration to OPM's identity and credit protection contractors, although it is not clear that the cases were related to the breaches.

By David Tobenkin



BREACH





- Courts soon may rule on two union lawsuits, determining whether those affected can expect to receive any money from the federal government and an IT contractor to compensate for the harm they suffered.

- The FBI's investigation into who was behind the breaches remains open, despite a claim by the Chinese government that it apprehended the criminals involved.

- Under new management prompted by the data breaches, OPM reports progress in addressing longstanding weaknesses in the agency's cybersecurity processes and procedures.

PROVIDING PROTECTION

OPM announced two separate breaches in 2015: One, disclosed June 4, involved 4.2 million individuals whose personnel file information was disclosed. Another, disclosed July 9, involved 21.5 million individuals whose security clearance and background check records were compromised. Together, the two breaches affected 22.1 million individuals, due to the overlap between the groups.

OPM offered those affected by the incidents similar forms of credit and identity theft protection – from contractor CSID, in the case of the personnel files breach, and contractor ID Experts, in the case of the background investigations breach. Protection under both forms includes identity monitoring, credit monitoring, identity restoration service, and identity theft insurance.

NARFE and other federal employee advocates lobbied strongly to have OPM offer lifetime credit monitoring and identity theft protection to those affected by the breaches, noting potential exposure to harm will continue long into the future.

In December 2015, President Obama signed into law the Consolidated Appropriations Act for FY 2016 (Public Law 114-113), which, in section 632, directs OPM to provide “complimentary identity protection coverage” at least as comprehensive as the coverage previously offered to the individuals affected by either hack for a period of not less than 10 years and to provide \$5 million in identity theft insurance for each victim. OPM is currently working on how best to incorporate

the additional coverage provided by the legislation, says an OPM spokesperson.

“NARFE’s priority remains lifetime coverage for those affected by the breaches,” says Jessica Klement, NARFE legislative director. “However, with Congress extending coverage to 10 years, it’s likely that it considers its job done in this regard.” NARFE is watching to see how the 10-year extension works, including seeing that the contract is awarded competitively and that all affected individuals are covered. “If threats still linger when we approach the 10-year mark, NARFE undoubtedly will work to extend coverage,” Klement adds.

Usage of the CSID and ID Experts services to date appears to be limited. OPM reports that, as of March 2016, of the 4.2 million employees affected by the personnel records breach, only 1,078,717 had taken advantage of the offered services. And of 21.5 million affected by the background investigation breach, OPM reports that only 2,610,740 have taken advantage of the services.

Of the NARFE members responding to a *narfe* magazine survey, some reported difficulties using the services or lack of responsiveness by the contractors. Others question why they are receiving seemingly unrelated information, such as updates regarding registered sex offenders in their area. And others appear satisfied with their service.

Many called for protection to be extended to family members whose sensitive data also was included in the records that were breached and who are, therefore, subject to potential fraud. An OPM spokesperson explained that protection is being provided to individuals whose Social Security numbers were compromised, which includes current and former employees and individuals whose Social Security numbers were somehow collected from other individuals, such as during background checks.

There are other areas in which NARFE is pushing for further action. “NARFE still has a major concern with the requirement that in order to sign up for the identity theft protection, individuals are required to have an email address,” says David Snell, director of NARFE’s Federal Benefits Service Department. “NARFE feels this requirement excludes those with certain disabilities from being able to take advantage of the monitoring offers, and we have sent a letter to OPM Acting Director Beth Cobert stating our

concerns and asking for OPM to provide an alternative to the blind/disabled.” An OPM spokesperson said that the agency is working with its service providers to provide a mailed option for alerts and reports.

THOUSANDS REPORT HARM

As of March 2016, 1,221 individuals affected by the personnel records breach had opened identity theft restoration cases, claiming that they had been victims of identity theft, says OPM spokesperson Sam Schumach. Another 5,503 identity restoration cases were opened by those affected by the background investigations incident.

There have been two identity theft insurance claims filed in connection with the personnel records incident, though neither of the claims has been paid out because the discovery of fraud was before the effective date of the policy, says Schumach, adding that no insurance claims have been filed with respect to the background investigations incident.

There “is no indication from law enforcement officials that suggests misuse of the information that was taken from OPM’s systems,” says Schumach. He notes that requests for identity restoration services may reflect incidents unrelated to the OPM data breaches. “Individuals are eligible to receive identity theft restoration services regardless of whether the identity theft is related to or traceable to the OPM breach,” he explains.

A total of 56 NARFE members responding to the *narfe* magazine survey said they had experienced identity theft or credit fraud since the OPM data breaches occurred, though many noted they had been affected by other data breaches in addition to those of OPM, leading some to say it was unclear which breach or breaches caused the harm.

A March 2016 amended class action complaint (amended complaint) against OPM and an IT security contractor, KeyPoint Government Solutions, Inc., listed among the plaintiffs 21 individuals reporting credit or identity related incidents against them that they believed were linked to the OPM data breaches. Among the incidents reported by those affected by the breaches were fraudu-

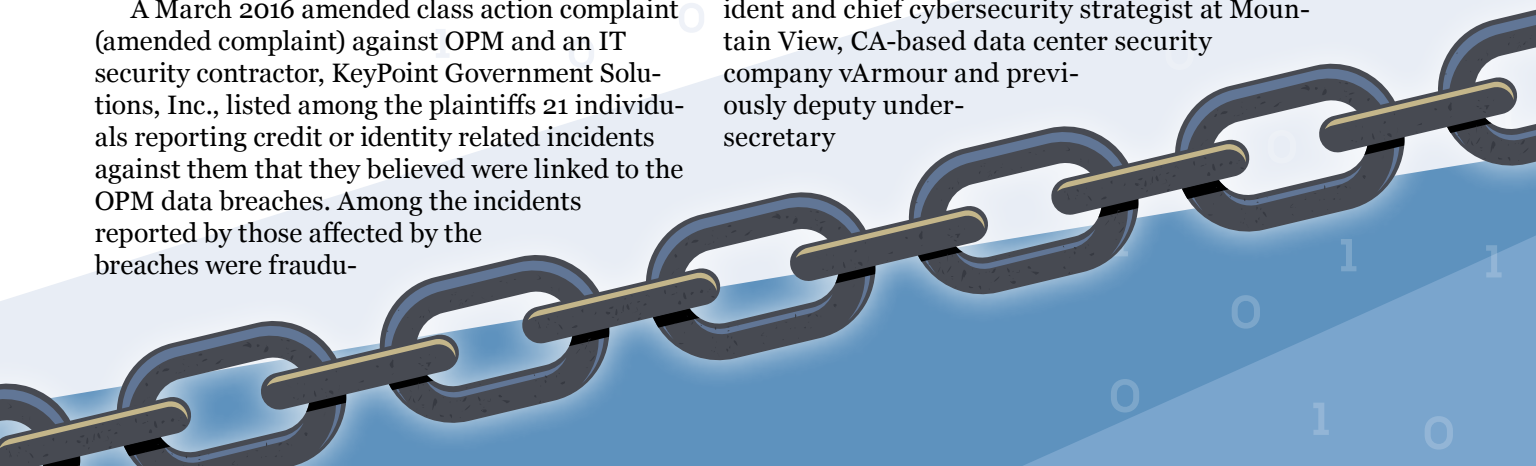
The full extent of the harm will not be known for years, given that the data will be useful to criminals and foreign espionage agents for a long period.

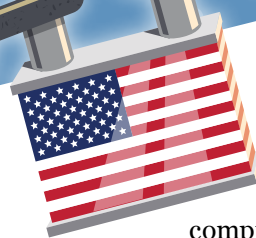
lent tax returns, unauthorized charges using credit information, notifications from the Social Security Administration of third-party attempts to use Social Security numbers, notification of findings of data on World Wide Web locations used by criminals, difficulties confirming identity due to fraudulent rival claims, fraudulent credit card accounts opened in their name, and fraudulent accessing of utility accounts.

On the other hand, some employee advocates say that they have not received numerous reports of harm. “We’re not hearing from a lot of members about identity theft or credit fraud – maybe from five members total,” says William R. Dougan, national president of the 110,000-member National Federation of Federal Employees.

Dougan and many experts said, however, that the full extent of the harm will not be known for years to come, given that the disclosed information will continue to be useful to criminals and foreign espionage agents for a long period.

“That [background investigations] data breach is the worst ever – I can’t imagine anything worse,” says Mark Weatherford, senior vice president and chief cybersecurity strategist at Mountain View, CA-based data center security company vArmour and previously deputy under-secretary





for cybersecurity at the U.S. Department of Homeland Security (DHS).

“It’s the worst because of the nature of the data compromised. The Questionnaire for National Security Positions [SF-86] questions are designed to make sure that if people have any skeletons in their closets, they will be reported there.”

VICTIMS’ DAY IN COURT

In June 25, 2015, the American Federation of Government Employees (AFGE) union and other plaintiffs filed a complaint against OPM and KeyPoint Government Solutions, Inc., a contractor that conducts background investigations for the government and from which the data breachers stole a credential to open OPM systems. That class action lawsuit, which was consolidated with others, alleges in the amended complaint that OPM failed to comply with the Federal Information Security Modernization Act of 2002 and 2014 (FISMA), violated the Privacy Act of 1974, and that it and KeyPoint engaged in other actionable misconduct.

The amended complaint seeks monetary damages for class members; indemnification of members from economic injury from the data breaches; lifetime identity theft and fraud protection to class members; and for OPM to formulate, adopt and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA, by, among other things, mandating that all unauthorized information systems be shut down and validly authorized before being reactivated. In March 2016, the complaint was amended to add new examples of harm. Another separate lawsuit that has been filed by the National Treasury Employees Union (NTEU) seeks remedies for NTEU members allegedly affected by the OPM data breaches.

In May, the government was expected to file motions to dismiss the amended complaint and the NTEU complaint, the first time in which the government will argue its side of the lawsuits.

All in all, class members affected by the data breach have a fairly strong case for recovery, given years of reports by OPM’s inspector general (IG) describing material weaknesses in OPM’s cybersecurity programs and processes and the IG’s documentation of a failure by OPM management to act upon such reports, says John Mahoney, a Wash-

ington, DC-based federal government employment lawyer and former federal administrative judge who has represented federal employees in Privacy Act cases.

“This is an unprecedented case that seems supported by FISMA and the Privacy Act,” Mahoney says. “The only issue is if OPM can contend that the data breaches were caused by an intervening criminal act, not by OPM. If the plaintiffs can get around that by arguing that OPM showed reckless disregard – and I think the government’s inaction in the face of years of reports by the OPM inspector general showing material weaknesses in their cybersecurity practices and noncompliance with federal cybersecurity law may rise to that level – they likely can get past the government’s defense.”

Chris K. Hikida, an associate for San Francisco-based law firm Girard Gibbs LLP, which is bringing the amended complaint, says that other individuals who were affected by the breach who are not named in the lawsuit will have a window to participate in the lawsuit if it is not dismissed. An OPM spokesperson said the agency could not comment on matters involving an active lawsuit.

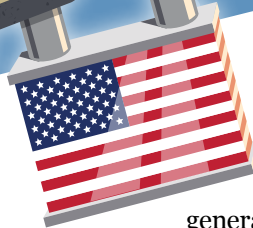
APPREHENDING THOSE RESPONSIBLE

When asked about the status of the investigation into the breaches, OPM and DHS spokespersons referred questions on the investigation to the FBI. The FBI confirmed in a statement that the investigation is outstanding but said little more.

In December 2015, *The Washington Post* reported that the Chinese government had announced that it had apprehended those responsible for the breaches and said that they represented criminals rather than state intelligence operatives. However, U.S. government officials declined at the time to publicly evaluate the Chinese assessment.

A NEW CYBERSECURITY REGIME

OPM has taken a number of steps following the data breaches to create a new cybersecurity regime for federal records. In June 2015, OPM released a Cybersecurity Action Report, announcing steps to improve IT security. Among these were increasing use of two-factor authentication (requiring two types of identification) for network access, reducing privileged users on the agency’s networks, and



trippling investment in IT modernization efforts. However, in November 2015, OPM's inspector general released an audit that found numerous cybersecurity shortcomings at the agency remained.

In January 2016, the Obama administration and OPM announced changes to address the safeguarding of the most sensitive data, that pertaining to background checks. OPM is creating a new governmentwide service provider for background investigations, the National Background Investigations Bureau (NBIB), which will be housed within OPM.

The Department of Defense (DOD), with its unique national security perspective, will design, build, secure and operate the NBIB's investigative IT systems in coordination with the NBIB. "Given how sensitive the data is and the impressive abilities of DOD in that area, I think leveraging that expertise makes sense," says Richard Spires, former DHS chief information officer and now chief executive officer of Herndon, VA-based IT and management training provider Learning Tree International, Inc.

In February 4, 2016, testimony before the Senate considering her confirmation as the new OPM director, Acting Director Cobert said OPM hopes to "have NBIB's initial operating capability officially established with a new organizational design and leader by October 2016."

Cobert also reported that OPM had made "significant progress" on improving the agency's cybersecurity, pointing to the requirement for two-factor authentication for network access, a strengthening of perimeter protections with firewalls, and installation of tools to better inspect incoming and outgoing traffic and create more visibility on the network. "I have also hired a Senior Advisor for Cybersecurity, to bring private-sector experience on how best to strengthen OPM's IT systems, modernize our IT infrastructure, and enhance the security of valuable federal IT systems and information," she said.

"At the same time, we have reorganized our Office of the Chief Information Officer, brought in a new Acting Chief Information Security Officer, and hired four new SES-level employees and four new senior IT program managers to further strengthen our senior IT team. On the process front, we are

putting into practice a new incident response plan, and OPM periodically requests independent penetration testing from our interagency partners."


OPM's fiscal year 2017 budget request includes \$37 million to enable it to continue efforts to migrate its existing legacy network to a new IT infrastructure (the "Shell"), which OPM contends will be more modern and more secure.

Some members of Congress, IT experts such as Spires, and the November 2015 IG audit report have expressed concerns that pursuing that ambitious program could be unwise, given past difficulties OPM has had implementing IT modernization programs, such as digitizing retirement claims processing, and the danger such efforts could divert energy from expeditious efforts to remedy the most pressing current IT security shortcomings.

However, in his February 2016 resignation notice to President Obama, OPM Inspector General Patrick McFarland, long critical of the agency's cybersecurity efforts, praised Cobert's efforts to date to improve cybersecurity.

Still, Spires says that the challenges pointed out in the OPM IG reports are so profound and extensive that it will take years for them to be worked out.

"Some of the issues highlighted in the November [2015] IG report are a decade in the making," says Spires. "When you have an organization with 23 major systems without authorizations, this shows an organization that was not focused on IT security in a way that it ideally should have been. On the other hand, under Beth Cobert, OPM seems to be addressing their shortcomings seriously and are getting their arms around the challenge. But to think you are going to fix it quickly is simply not realistic. You need a five-year plan to address challenges of this magnitude. My sense is that they are taking significant steps that you are not seeing the fruits of yet."

External assessments of how much progress has been made will come soon. Later this year, the Government Accountability Office (GAO) will release a comprehensive examination of OPM's efforts to reduce the risk of future data breaches that was directed by Congress, says Greg Wilshusen, director of information security issues at GAO. 

—DAVID TOBENKIN IS A FREELANCE WRITER BASED IN THE GREATER WASHINGTON, DC, AREA.