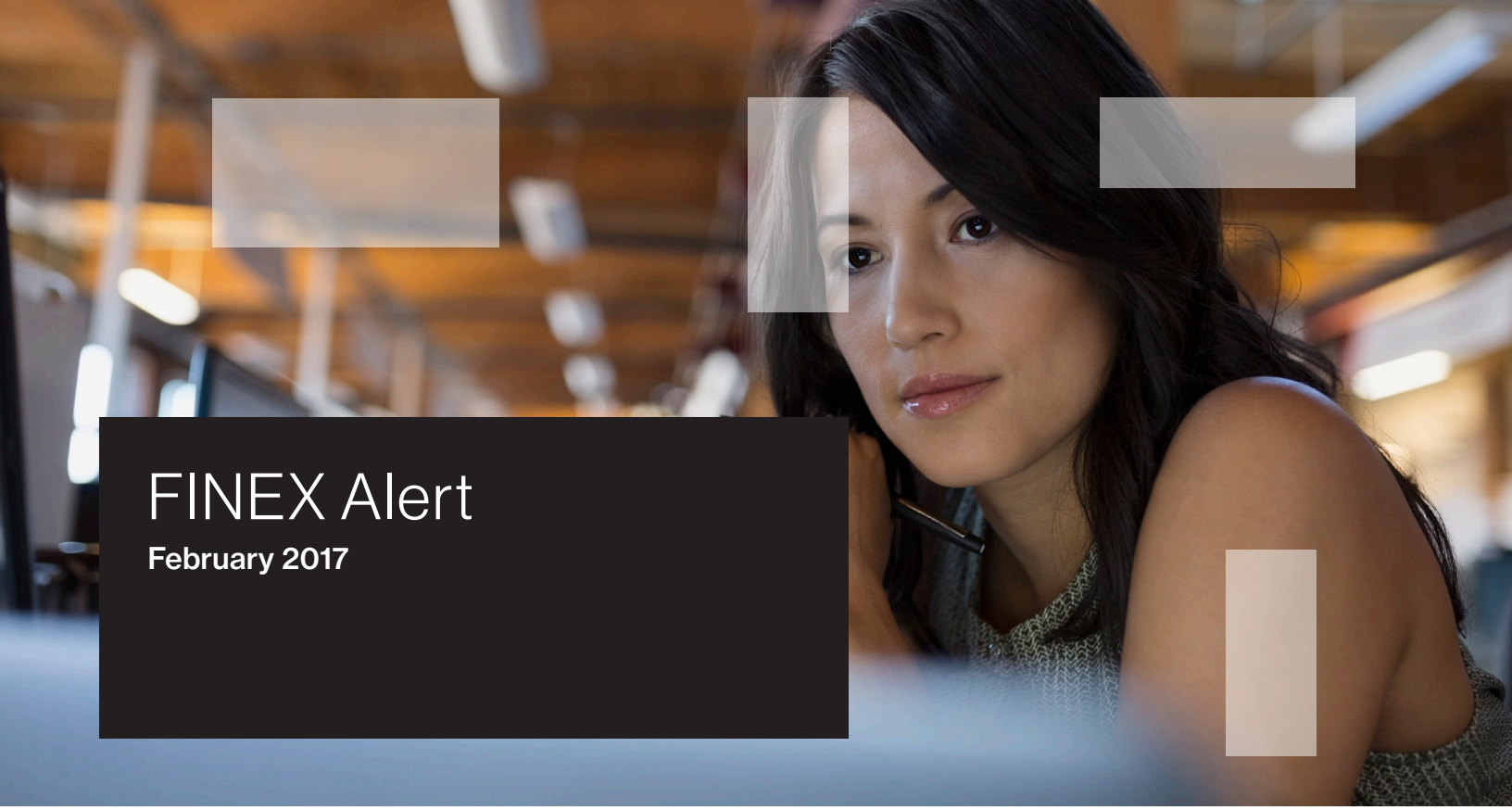


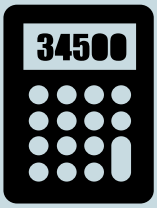
FINEX Alert

February 2017

A seasonal cyber exposure — Increasing awareness to reduce tax return fraud

The potential for cyber breaches remains a constant throughout the year. Some breaches, however, are more prevalent during certain seasons. For example, retailers face higher exposure during the holidays, and airlines and hospitality organizations may see increased breach activity during peak travel seasons, due to increased customer volume.

One seasonal cyber exposure impacting all industries occurs during tax filing season (January – April) because of the manner in which tax forms are transmitted and the ability of identity thieves to file and receive fraudulent tax returns. There are many opportunities for fraud during the creation, delivery and usage of tax documents, including while that information is under the care, custody and control of the employer or its vendors. These types of fraud affecting businesses generally follow a common pattern. For example, an employee or vendor whose responsibilities include access to payroll and related tax data could be a victim of a phishing attack whereby they unknowingly grant access to employees' personally identifiable information (PII) to unauthorized persons. Most commonly, the fraudsters are then able to prepare and file tax returns with the stolen PII, subsequently stealing employees' refunds (although there are other ways the data can be monetized). Furthermore, the fraud generally isn't detected for a while given the time lag between the compilation of the W-2 forms and processing of returns. Of note for this type of incident is that the typical remedies offered to individuals impacted by a cyber breach, mostly commonly credit monitoring, would not detect this type of fraud. Credit monitoring is generally designed to detect a variety of



One seasonal cyber exposure impacting all industries occurs during tax filing season because of the manner in which tax forms are transmitted and the ability of identity thieves to file and receive fraudulent tax returns.

suspicious activity impacting a credit report but not to alert an individual when taxes have been filed or refunds have been disbursed in his/her name.

A noteworthy case from the 2014 filing season involved a university medical center when the PII of more than 60,000 employees was accessed and of which 953 were used to file fraudulent tax returns. Thieves attempted to file $2.2 million in tax returns and received $1.4 million before the fraud was detected and stopped by the Internal Revenue Service (IRS). Personal tax filing software and proxy servers were used to mask the location of the filers, making it appear that the filers were located in the jurisdiction where the hack occurred. The funds were then used to buy online gift cards for goods sent to Venezuela. In mid-2016, a Venezuelan national in Cuba was arrested and extradited to the United States and charged with conspiracy to defraud the United States, wire fraud, money laundering and aggravated identity theft. While it is promising when identity thieves are caught, too often the perpetrators are not and are able to move on to the next victim.

IRS advisory to organizations

In March 2016, the IRS warned that phishing attacks had increased 400% over the previous year. While it is too early to determine the activity for the 2016 filing season, the IRS also recently concluded a week-long effort – the National Tax Security Week – to inform the public of the risk of identity theft and fraudulent tax returns. Considerable efforts have been made by both the public and private sectors, leading to over $4B of fraudulent returns halted d by the IRS fraud detection systems the first nine months of 2016. For example, an Information Sharing and Analysis Center (ISAC) specifically dedicated to identity tax fraud will launch in 2017, and a pilot program requiring additional verification on W-2 will be expanded to a larger taxpayer population for the 2016 filing year.

Reducing incidents of tax return fraud

The government continues to increase awareness and dedicate resources to addressing the risk, but attackers remain one step ahead of technology, creating a significant exposure to organizations across industries and size. As such, the way organizations are exposed to cyber incidents is constantly evolving, requiring vigilance, diligence and a culture of awareness that extends beyond the traditional four corners of an employee's job responsibilities.

The good news is that many of the efforts organizations are dedicating to information security and data privacy can help protect their employees from tax fraud and, consequently, prevent potential liability for privacy violation or negligence lawsuits (and other types of claims) by employees if their data and refunds are stolen. Although cyber liability insurance can address most of this exposure, equally important are advanced malware detection, phishing exercises and employee training in addressing the risks of this type of cyber incident. Even more important is an organizational culture that encourages awareness, responsibility and accountability for information security and data privacy – so that the individual employee's effort creates a powerful detection and monitoring tool in the aggregate.

For additional information about this Alert, please contact your Willis Towers Watson Client Relationship Director or emily.lowe@willistowerswatson.com.

Contact

Emily Lowe
Vice President
FINEX Cyber Practice
+1 617 351 7485
emily.lowe@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 territories. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Willis Towers Watson