LANSING CHAPTER OF THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

2024 LACFE Board Election Results

Mark Lee, Nanci Bashore, Jen Ostwald and Jennifer Edmonds were all re-elected. Thanks for voting!

At the Annual Meeting on August 28th, officers were elected and each board member will continue to serve in their present capacity. This year, we hosted a networking event following the Annual Meeting at the Lansing Shuffle. If you missed this event, be sure to catch our next networking!

Less happy news… the articles/speech I featured this month each contain disheartening information about cyber attacks and ways technology is being exploited to harm individuals and steal their private information.

As fraud examiners, we know to be aware of and protect ourselves and others from these types of risks, but we must keep vigilant in our efforts. As we also know, the criminals are also working hard to profit from any missteps.

In This Issue

Fraud Talk Podcast

Fraud Prevention and Program Integrity in the Public Sector - Amanda Holden - Fraud Talk - Episode 147

Amanda Holden, a partner with Deloitte's Financial Crimes, joins Samuel May, ACFE research specialist, on Fraud Talk to uncover the intricacies of fraud prevention and program integrity in the Canadian public sector. They navigate the crucial role of proactive prevention and detection, addressing the unique challenges faced by public entities in a rapidly evolving fraud landscape. Holden explores the essential COSO framework, emphasizing the balance between expediency and robust fraud controls. Dive into Holdens's expert insights on breaking down cultural barriers, enhancing information sharing and leveraging cutting-edge data analytics and technology.

https://acfe.podbean.com/e/fraud-prevention-and-program-integrity-in-the-public-sector-amanda-holden-fraud-talk-episode-147/

UPCOMING EVENTS

LOCAL:

LACFE Fall Training – Steven Kohn "Rules for Whistleblowing"
October 17, 2024
Lansing, Exact location TBD.
Pricing TBD
Each attendee with receive a copy of the book! More information to follow soon!

ACFE South East Michigan Chapter Dinner Meeting/Training
Monthly In Person, beginning September 5, 2024
5:30 – 8:30 PM
St. John's Banquet & Conference Center
22001 Northwestern Highway
Southfield, MI 48075
Learn more: https://semcacfe.org/meetinginfo.php?id=100&ts=1723475853

ACFE Southwest Ohio Chapter: AI, Accounting, Ethics, and Fraud Threats
In Person/Virtual
September 13, 2024
12:00 PM - 2:00 PM
Learn more: https://swohacfe.org/events

MICPA Advance
In Person
November 20, 2024
8:30 am - 5:00 pm
MSU Management Education Center Troy, MI
Learn more: https://www.micpa.org/cpe/store/course-detail?ProductId=160169&return=3~1

NATIONAL:

ACFE Revolutionizing Fraud Fighting: Boosting Productivity with AI and ChatGPT
Virtual Seminar
September 10, 2024
Learn more: Event Details (acfe.com)

ACFE Self-Study Auditing CPE Bundle
Earn up to 20 Continuing Professional Education (CPE) credits with a curated bundle of self-study CPE courses focused on auditing. With this bundle you can save more than 50% vs. purchasing the courses individually. All courses provide NASBA-approved CPE and can be used for other professional credentials.
Learn more: Product Detail Page (acfe.com)

Help me create your newsletter! If you have an event that you would like posted or if you wish to share an article or job opening, please contact Jennifer Ostwald at newsletter@lansingacfe.com

McLaren Health Care systems restored after weeks of disruption from ransomware attack

August 27, 2024
Kristen Jordan Shamus
https://www.freep.com/story/news/health/2024/08/27/mclaren-health-care-ransomware-attack-2024-cyberattack/74959099007/

McLaren Health Care said its technology platforms have been fully restored following an Aug. 5 ransomware attack that disrupted operations at all 13 of its hospitals, surgery, infusion and imaging centers, along with its network of 113,000 medical providers throughout Michigan, Indiana and Ohio.

"All temporary procedures enacted during the disruption have been lifted," McLaren said in a statement issued Monday. "Providers at all McLaren Health Care hospitals, Karmanos cancer centers, and outpatient clinics again have access to patients’ electronic medical records."

Appointments now can be scheduled and surgeries that were postponed during the ransomware attack are now being rescheduled, the health system said.

"We have been largely operational for some time, and our staff has been reaching out to patients for the past couple of weeks to reschedule appointments impacted by the event," said David Jones, a McLaren spokesperson.

It could be a few more weeks, however, before details about medical care that took place over the last three weeks will be visible in patients' electronic charts. That's because McLaren staff will have to manually input lab and imaging test results, notes from office visits, surgeries, and other care that occurred during the tech disruption. It's a process that began over the weekend "and is expected to last several weeks," McLaren said.

Patients told the Free Press earlier this month that the ransomware attack led to the cancellation of cardiac tests and radiation treatments for cancer during the tech disruption. Some ambulances were diverted from McLaren hospitals and appointments had to be canceled because physicians couldn't access radiology reports, lab test results or orders for additional testing and procedures.

Some hourly employees told the Free Press that McLaren required them to use up all their paid time off during the tech disruption, and when that ran out, they went unpaid.

This was the second ransomware attack at Grand Blanc-based McLaren within a year. A ransomware gang known as BlackCat/AlphV claimed responsibility for another crippling tech disruption that began in August 2023. The group claimed in a post online that it stole 6 terabytes of data, including the personal information of 2.5 million patients.

McLaren reported at the time that it had shut down its own computer networks "out of an abundance of caution" after its information technology security team found suspicious activity during routine monitoring.

It's still unclear whether the latest McLaren ransomware attack led to a breach of protected personal or health data about patients or employees.

"McLaren is continuing its work with cybersecurity experts to determine what, if any, patient or employee information was compromised," the health system said. "If it is determined that any protected health information (PHI) or personal information was compromised, those individuals will be contacted directly."

McLaren isn't alone in dealing with the fallout of cybercriminals in the health care sector.

In May, 140 Ascension hospitals in the U.S. were struck by a cyberattack, cutting off electronic access to medical records, lab test results, radiology imaging and even impaired the ability for doctors to issue medical orders. At Ascension's Michigan hospitals, ambulances were diverted and there were hours long delays in treating even critically ill patients, employees told the Free Press.

Also in May, the personal information of more than 56,000 people — including names, medical record numbers, addresses, dates of birth, diagnostic and treatment information, and health insurance details — was compromised in a cyberattack at Michigan Medicine, the academic medical center of the University of Michigan.

From 2018-22, there was a 93% rise in large cybersecurity breaches reported to the U.S. Department of Health and Human Services Office for Civil Rights and a 278% increase in large breaches involving ransomware, the agency reported.

These breaches can cause disruptions to the care of patients, delay medical procedures and put patient safety at risk.

“Our experience has made clear that cyberattacks against our health care infrastructure are an industrywide problem, and it’s not hyperbole to call health care cybercrime a national security threat," said Phil Incarnati, president and CEO of McLaren, in a statement issued earlier this month.

“I’m committed to working with my fellow providers, elected officials, law enforcement and cyber experts to find ways to hold these criminals accountable and prevent their entry into our systems."

Attorney General Merrick B. Garland Delivers Remarks on the Justice Department’s Lawsuit Against RealPage for Algorithmic Pricing Scheme that Harms Millions of Americans

August 23, 2024
https://www.justice.gov/opa/speech/attorney-general-merrick-b-garland-delivers-remarks-justice-departments-lawsuit-against

Good morning.

Over a century ago, Congress passed the Sherman Antitrust Act to protect competition in the marketplace. As the Supreme Court has explained, the “central evil” addressed by Section 1 of that Act is “the elimination of competition that would otherwise exist,” including competition on prices.

When the Sherman Act was passed, an anticompetitive scheme might have looked like robber barons shaking hands at a secret meeting.

Today, it looks like landlords using mathematical algorithms to align their rents.

But antitrust law does not become obsolete simply because competitors find new ways to unlawfully act in concert.

And Americans should not have to pay more in rent simply because a company has found a new way to scheme with landlords to break the law.

So today, after a nearly-two-year investigation, the Justice Department, joined by eight states, has sued RealPage, a commercial real estate software company, for violating the Sherman Antitrust Act.

RealPage sells landlords what it calls “revenue management” software. We allege that this software is developed, marketed, and sold to enable landlords to sidestep vigorous competition in the rental market. Competing landlords agree to submit to RealPage, on a daily basis, their most sensitive, non-public information, including rental rates, lease terms, and projected vacancies.

RealPage then combines this data from competing landlords and feeds it into an algorithm that provides real-time pricing recommendations back to the competing landlords.

But as we allege, these are more than just recommendations. RealPage actively polices landlords’ compliance with those recommendations. It also monitors landlords’ other policies by, for example, trying to stop concessions that landlords use to attract or retain renters.

A large number of landlords effectively agree to outsource their pricing decisions to RealPage by using an “auto accept” setting, which effectively permits RealPage to determine the price a renter will pay.

Landlords understand what their arrangement with RealPage gets them. As one said, “I always liked this product because your algorithm uses proprietary data from other subscribers to suggest rents and terms. That’s classic price fixing.”

And RealPage understands what it’s doing, too. In advertising its service to landlords, RealPage frequently says that a “rising tide raises all ships.” As a RealPage vice president explained, this phrase means that “there is greater good in everybody succeeding versus essentially trying to compete against one another.”

But “essentially trying to compete against one another” is what our free-market economy is all about. And ensuring such competition what our antitrust laws are all about.

Americans spend more money on housing than any other expense. Tens of millions of Americans are renters, and almost half of those households spend close to a third of their hard-earned income on rent.

Under the antitrust laws, landlords — like any competitors — may not share with each other their confidential, sensitive data in a way that permits them to align how they price their products —in this case apartments — and thus cause renters to pay more than they would in a competitive market. Using software as the sharing mechanism — or calling it “Artificial Intelligence Revenue Management” as RealPage does — does not immunize the scheme from Sherman Act liability.

The Justice Department takes seriously its responsibility to protect Americans from illegal conduct that undermines competition and drives up prices.

We will continue to aggressively enforce the antitrust laws and protect the American people from those who would violate them.

I applaud the attorneys and staff of the Department’s Antitrust Division for their outstanding work on this case on behalf of the American people.

Thank you all.

Video of the Month

Criminals Steal Couple’s Credit Card Points... It's Possible! (youtube.com)

The Perfect Scam
Jody and her husband love to travel, and they love to save up credit card reward points to make their family vacations more affordable. When they start getting notifications that some of their points have been redeemed without their permission, they are led on a months long ordeal to secure their accounts from criminals who are turning those hard-earned points into cash.

AARP’s weekly podcast The Perfect Scam, a project of the AARP Fraud Watch Network, tells the stories of people who find themselves the target of a scam. Host Bob Sullivan introduces listeners to those who have experienced scams firsthand, as well as leading experts who pull back the curtain on how scammers operate.

Exploiting Chaos: How Fraudsters Capitalized on the 2024 CrowdStrike Falcon Sensor Outage

August 27, 2024
Samuel May
https://www.acfe.com/acfe-insights-blog/blog-detail?s=crowdstrike-outage-fraud

On July 19, 2024, CrowdStrike pushed out an update to one of its programs, a vulnerability scanning tool called Falcon Sensor, that contained a significant bug. For computers running on a Microsoft Windows operating system, this faulty update caused the computer to crash.

CrowdStrike is an American cybersecurity company that provides security software products, threat intelligence and cyberattack response services. Founded in 2011, CrowdStrike grew quickly and had its initial public offering on the Nasdaq in June 2019. By 2024, CrowdStrike had yearly revenues in the billions from their software products serving corporations the world over.

The Outage

On July 19, 2024, CrowdStrike pushed out an update to one of its programs, a vulnerability scanning tool called Falcon Sensor, which contained a significant bug. For computers running on a Microsoft Windows operating system, this faulty update caused the computer to crash. The systems would then be unable to reboot successfully, continually running into errors in the Falcon software and rendering the computer inoperable. Microsoft would later estimate that approximately 8.5 million devices were directly affected. Organizations across all variety of industries lost access to critical systems, including airlines, public transit systems in multiple cities, hospitals and clinics, financial institutions, and media outlets around the world. The total global cost is estimated in the billions of dollars. It is the largest information technology (IT) outage in history.

CrowdStrike purportedly identified the issue and deployed a fix within hours. Unfortunately, restoring individual computers required hands-on implementation, manually booting affected systems and remedying the issue. While most critical systems were repaired within a day, some organizations took significantly longer to fully recover.

The Opportunity

Despite the rapid response time and the availability of solutions directly from CrowdStrike and Microsoft, fraudsters smelled an opportunity. As is always the case with disasters, outages, tragedies and other well publicized events, malicious actors will find ways to try to take advantage of people already in distress. Easy similarities can be made to COVID pandemic fraud, natural disaster scams or even tax season fraud (which may not be a traditional disaster, but certainly results in many distressed citizens).

CrowdStrike recovery scams started immediately. In the days following the outage, CrowdStrike itself released information on identified spear phishing attempts. The company also released information on general malicious activity surrounding the event.

Fraud examiners will recognize these commonly used attacks: malicious emails, scam phone calls and fake websites targeting companies reporting outages and their employees. Fraudsters posed as technical support or CrowdStrike staff offering refunds or remuneration for losses caused by the outage. The well publicized outage gave fraudsters an easy list of targets. As organizations added themselves to the growing list of businesses and government agencies that were temporarily unavailable, they were also painting themselves, and their customers, with targets.

Emails were sent to known corporate addresses with malicious attachments. The emails posed as CrowdStrike, Microsoft or other technical support staff sharing important recovery information. An attached PDF promised to contain the method to restore crashed systems, or a download link promised to install a program that would protect as-yet unaffected systems. Websites were created within hours of the first major outage reports, using URLs similar to real CrowdStrike websites to steal information from unwary users or to host malicious software posing as solutions. Fake CrowdStrike social media sites cropped up, linking to malicious websites or asking for users to message the fraudsters posing as support through the social media platform.

While not as directly connected, frauds and scams targeted at customers of businesses affected by the outage also see an increase. For example, airlines affected by the outage began issuing refunds to customers whose flights were cancelled. Fraudsters posing as the airline, aware of the outage, identify customers on social media posting about delays, cancellations or venting their frustration in the public forum. The fraudster then provides links to fake websites, fake social media accounts or phishes with targeted emails, phone calls or instant messages, convincing the customer their refund is just a few clicks away, they just need to provide their credit card information to process the refund.

The Takeaway

These kinds of events are inevitable, and fraudsters will always look to take advantage of them. Unfortunately, even with sound and consistent anti-fraud training for organizations and individuals, disasters and stress limit our attention to detail and make us more susceptible to hasty actions. Fraud examiners must stay ahead of the wave, reacting to situations appropriately with timely reminders to remain cautious and to look for solutions or assistance through secure channels. These scams are usually quick and dirty, so remind staff, friends and family of their traditional cyber security scrutiny: check the URLs, email addresses and usernames and avoid clicking links or downloading attachments. It is easy to do on a well-caffeinated, calm morning at the office, but significantly harder when you are stranded after a flight cancellation, your bank’s website is down, and you are hastily scrolling for solutions.