Texas Public Funds Investment Conference

What’s Current in Payment Fraud
November 7, 2019

speaker:

Sandy Sullivan, CFE
Senior Vice President | Fraud Management
Frost Bank
(210) 220-5935 work | (210) 260-3759 mobile
ssullivan@frostbank.com
What we are seeing in the fraud arena......

- **BEC Fraud (Business Email Compromise Fraud) or EAC (E-mail Account Compromise)**
  - Companies of all sizes - any industry
  - Individuals
  - Real Estate/Property Management/Title Companies – huge targets
  - It is not always money they are seeking...sometimes it’s “Personally Identifiable Information” also known as “PII” such as....i.e. needing W9 information
  - Changing bank’s and/or account #’s for salary direct deposit
- Ransomware
- Elder Financial Exploitation – there is a tsunami coming down the road
- Commercial Customer employee embezzlement
- Check fraud
- Debit Card / Credit Card Fraud
- Spoofing of a bank’s telephone number and pretending to be someone from the bank...usually pretending to be someone in the fraud department or IT
- Spoofing other agencies such as the IRS; Social Security Administration; the Sheriff’s Office (Court Duty); Collection Agencies; etc.
- And many more too numerous to list......
Questions regarding this PSA should be directed to your local FBI Field Office.
Local Field Office Locations:  www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update and companion to Business E-mail Compromise (BEC) PSA 1-050417-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data for the time frame October 2013 to May 2018.

DEFINITION
Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.1

STATISTICAL DATA
The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between December 2016 and May 2018, there was a 136% increase in identified global exposed losses2. The scam has been reported in all 50 states and in 150 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 115 countries. Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom, Mexico and Turkey have also been identified recently as prominent destinations.
SUGGESTIONS FOR PROTECTION

BEC/EAC actors have been known to target all parties in a real estate transaction. The best defense is to verify all requests for a change in payment type and/or location. BEC/EAC actors often request that payments originally scheduled for check dispersal be made via wire instead. BEC/EAC actors may also request changes to the original recipient’s financial information.

BEC/EAC actors will use information that is publicly available on real estate listing sites to target victims. This may include homes that are for sale and the progress of the sale such as “under contract” as well as the contact information of the real estate agent. Be wary of any communication that is exclusively e-mail based and establish a secondary means of communication for verification purposes.

Be mindful of phone conversations. Victims have reported receiving phone calls from BEC/EAC actors requesting personal information for verification purposes. Financial institutions report phone calls acknowledging a change in payment type and/or location. Some victims report they were unable to distinguish the fraudulent phone conversation from legitimate conversations. One way to counter act this fraudulent activity, is to establish code phrases that would only be known to the two legitimate parties.

Title Companies report establishing new procedures when processing legal documents requiring all changes in payment type and/or location to be verified prior to distributing funds.

If you discover a fraudulent transfer, time is of the essence. First, contact your financial institution and request a recall of the funds. Different financial institutions have varying policies; it is important to know what assistance your financial institution will provide when attempting to recover funds. Second, contact your local FBI office and report the fraudulent transfer. Law enforcement may be able to assist the financial institution in recovering funds. Finally, regardless of dollar loss, file a complaint with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov. The IC3 will be able to assist both the financial institutions and law enforcement in the recovery efforts.
September 10, 2019
Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local FBI Field Office.
Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION
Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.
The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.
The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees’ Personally Identifiable Information or Wage and Tax Statement (W-2) forms.

STATISTICAL DATA
The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.
The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between October 2013 and July 2019:

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019:**

<table>
<thead>
<tr>
<th>Domestic and international incidents:</th>
<th>166,349</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic and international exposed dollar loss:</td>
<td>$26,201,775,589</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>The following BEC/EAC statistics were reported in victim complaints to the IC3 between October 2013 and July 2019:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total U.S. victims:</td>
</tr>
<tr>
<td>Total U.S. exposed dollar loss:</td>
</tr>
<tr>
<td>Total non-U.S. victims:</td>
</tr>
<tr>
<td>Total non-U.S. exposed dollar loss:</td>
</tr>
</tbody>
</table>
The IC3 participates in multiple initiatives targeting an array of cyber crime schemes that victimize individuals and businesses domestically and abroad. These initiatives are a coordination of industry resources along with the investigative resources provided by cyber crime task forces comprised of federal, state, and local law enforcement agencies. The success of these initiatives is directly attributable to the inclusion of the industry resources. Initiatives focus on the following:

- Charitable Contributions Fraud
- Counterfeit Check Fraud
- Identity Theft Task Force
- International Fraud
- Investment Fraud
- Online Pharmaceutical Fraud
- Phishing
- Work-at-home scams

2014 IC3 Statistics:

3,175,611 Complaints Reported to IC3 Since Inception

Total Complaints Received in 2014: 269,422

Complaints Reporting a Loss: $23,084

Total Losses Reported: $800,482,373

Median Dollar Loss for Complaints Reporting a Loss: $330

Average Dollar Loss Overall: $9,511

Average Dollar Loss for Complaints Reporting a Loss: $9,472

IC3 Complaints by Year:

- 2010: $133,869
- 2011: $134,294
- 2012: $299,974
- 2013: $232,812
- 2014: $209,422

Number of Visitors to www.ic3.gov Website: 552,135,205

www.ic3.gov
AN INVESTIGATIVE LOOK INTO THE IC3

Mission of the IC3:
The mission of the Internet Crime Complaint Center (IC3) is to provide the public with a reliable and convenient reporting mechanism to submit information to the Federal Bureau of Investigation concerning suspected Internet-facilitated criminal activity and to develop effective alliances with industry partners. Information is processed for investigative and intelligence purposes for law enforcement and public awareness.

The IC3 Alliances:
The IC3 Unit is part of the Cyber Division’s Cyber Operations Section V within the FBI. The IC3 Unit is staffed by FBI agents and professional staff employees with expertise in the prevention, detection, and investigation of cyber crime.

The IC3 has formed additional alliances with industry representatives (e.g. online retailers, financial institutions, Internet service providers, and parcel delivery providers) that have exponentially increased the flow of the IC3’s most valuable commodity - INFORMATION. Working with federal, state, local, and international law enforcement, as well as regulatory agencies, IC3 analysts receive, develop, and subsequently refer information for investigative and prosecutive attention.

Cyber Crime and the IC3:
As technology evolves, so do the many methods used to exploit technology for criminal purposes. Nearly all crime that once was committed in person, by mail, or over the telephone can be committed over the Internet. The criminal element is empowered by the perceived anonymity of the Internet and the ease of access to potential victims. Criminals use social engineering to prey on their victims’ sympathy, generosity, or vulnerability. The IC3 was designed to help address all types of cyber crime through its complaint system.

IC3 Complaints:
The complaints submitted to the IC3 cover an array of cyber crime including theft of intellectual property rights, computer intrusion, economic espionage, online extortion, and international money laundering. Numerous fraud schemes such as identity theft, phishing, spam, reshipping, auction fraud, payment fraud, counterfeit goods, romance scams, and non-delivery of goods are reported to the IC3.

Searching the IC3 Database:
The IC3 recently expanded the remote search capabilities of the IC3 database making it available to all sworn law enforcement and FBI personnel through the Law Enforcement Enterprise Portal (LEEP). Users can connect directly to the IC3 Complaint Search after authenticating through LEEP from the user’s Identity Provider (IDP) or through the user’s Law Enforcement Online membership at www.leo.gov. Users may also contact the IC3 for analytical assistance. While developing a case in the database, Management and Program Analysts compile similar complaints, collect relevant case information from both open-and-closed source public information databases and confer with federal, state, local and international law enforcement personnel. The IC3 compiles this information into reports that are available to all law enforcement.

Public Service Announcements:
The IC3 prepares public service announcements on the latest cyber trends to alert consumers on Internet fraud. These announcements are posted on the following Web sites:

www.ic3.gov
www.fbi.gov
The FBI’s Internet Crime Complaint Center (IC3) received nearly 352,000 complaints related to cybercrime activity that collectively was responsible for $2.7 billion in losses.

Despite being only the sixth most commonly reported cybercrime in 2018, BEC/EAC campaigns was the top crime with the highest reported loss total: nearly $1.3 billion. In particular, the IC3 took note of an increase in the number of these scams that used spoofed emails, texts or phone calls to trick victims into thinking a superior or authority figure asked them to purchase gift cards.

To combat the growing BEC plague, IC3 last year launched its Recovery Asset Team, which “works within the Domestic Financial Fraud Kill Chain (DFFKC) to recover fraudulent funds wired by victims,” the annual report explains. “The DFFKC is a partnership between law enforcement and financial entities. In 2018, the IC3 RAT notified 56 field offices and 12 legal attachés of 1,061 DFFKCs totaling $257,096,992, a recovery rate of 75 percent.”
The report also noted some standout or emerging trends from the past year. These included:

- Payroll diversion scams, in which cybercriminals use phishing emails to capture employees’ login credentials in order to access their payroll accounts and redirect their direct deposit payments to an attacker-controlled account. The IC3 received about 100 such complaints, which were responsible for about $100 million of losses.

- Extortion. The report noted a 242 percent increase in extortion-related complaints since 2017, with adjusted losses of over $83 million.

- Tech support fraud. The FBI tracked a 161 percent year-over-year increase in losses resulting from such crimes. Altogether, victims from 48 countries lodged 14,408 complaints, with losses amounting to nearly $39 million.

The over-60 population represented the largest share of complaints and total losses. Outside of the U.S., the foreign country with the most reported victims was India (4,556), followed by the UK (3,970) and Canada (2,880).

The IC3 says its received a total of roughly 4.42 million complaints since its inception in 2000.
Ransomware is a form of malware that targets both human and technical weaknesses in organizations and individual networks in an effort to deny the availability of critical data and systems. Ransomware is frequently delivered through spear phishing e-mails to end users. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor will purportedly provide an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.
Key areas to focus on with ransomware are prevention, business continuity, and remediation. As ransomware techniques continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity.

**Prevention Considerations**
- Implement an awareness and training program. Because end users are targeted, employees and individuals should be made aware of the threat of ransomware and how it is delivered.
- Patch operating systems, software, and firmware on devices, which may be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and that regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege: no users should be assigned administrative access unless absolutely needed; those with a need for administrator accounts should only use them when necessary.
- Configure access controls, including file, directory, and network share permissions, with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

**Business Continuity Considerations**
- Back up data regularly, and regularly verify the integrity of those backups.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, this may be the best way to recover your critical data.

**Other Considerations**
- Implement application whitelisting; only allow systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organizational units.

**The Ransom**
The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases the FBI encourages organizations to contact a local FBI field office immediately to report a ransomware event and request assistance. Victims are also encouraged to report cyber incidents to the FBI’s Internet Crime Complaint Center (www.ic3.gov).
REPORT TO THE NATIONS
2018 GLOBAL STUDY ON OCCUPATIONAL FRAUD AND ABUSE
KEY FINDINGS

2,690 real cases of occupational fraud
in 125 countries in 23 industry categories

$7 BILLION+ in total losses
$130,000 median loss per case
22% of cases caused losses of $1 MILLION+

Median duration of a fraud scheme
16 MONTHS

Corruption was the most common scheme in every global region

TIPS are by far the most common initial detection method

Internal audit 15%
Management review 13%

Employees provide over half of tips, and nearly 63% come from outside parties

Organizations with hotlines detect fraud by tips more often

$800,000 median loss

Asset misappropriation schemes are the most common and least costly

$114,000 median loss
89% of cases

Financial statement fraud schemes are the least common and most costly

15% of cases

$200,000 median loss

Small businesses lost almost twice as much per scheme to fraud

$104,000 median loss

Employees

$200,000median loss

Top reason for non-referrals was fear of bad publicity

-16%
HOTLINES AND REPORTING MECHANISMS

The presence of a hotline or other reporting mechanism affects how organizations detect fraud and the outcome of the case.

63% of victim organizations had hotlines

46% of cases detected by tip

30% of cases detected by tip

50% of cases detected by tip

46% of cases detected by tip

30% of cases detected by tip

CORRUPTION IS PARTICULARLY LIKELY TO BE DETECTED BY TIP

50% detected by tip

38% detected by tip

38% detected by tip

Fraud losses were 50% smaller at organizations with hotlines than those without.

Organizations without hotlines were more than twice as likely to detect fraud by accident or by external audit.

Telephone hotlines are most popular, but whistleblowers use various reporting mechanisms.

Telephone hotline: 42%

Email: 26%

Web-based/online form: 23%

Mailed letter/form: 16%

Other: 9%

Fax: 1%

NOT ALL TIPS COME THROUGH HOTLINES

When a reporting mechanism is not used, whistleblowers are most likely to report to:

Direct supervisor: 32%

Executive: 15%

Fraud investigation team: 13%

Coworker: 12%

Internal audit: 10%
FRAUD IN SMALL BUSINESSES

Fraud can be especially devastating to small businesses. These organizations typically have fewer resources to both prevent and recover from a fraud, and they often require an increased level of trust in employees due to a lower ability to implement robust anti-fraud controls.

SMALL BUSINESSES LOSE ALMOST TWICE AS MUCH PER SCHEME TO OCCUPATIONAL FRAUD

<table>
<thead>
<tr>
<th>&lt;100 EMPLOYEES</th>
<th>100+ EMPLOYEES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median loss</td>
<td>$200,000</td>
</tr>
<tr>
<td>Frauds detected by tip:</td>
<td>29%</td>
</tr>
<tr>
<td>Frauds caused by lack of internal controls:</td>
<td>42%</td>
</tr>
<tr>
<td>Frauds perpetrated by an owner/executive:</td>
<td>29%</td>
</tr>
</tbody>
</table>

Small businesses typically have fewer anti-fraud controls than larger organizations, leaving them more vulnerable to fraud.

Small businesses face different risks than larger organizations.

- Corruption: <100 employees 22%, 100+ employees 48%
- Billing: <100 employees 39%, 100+ employees 29%
- Cash and payment tampering: <100 employees 21%, 100+ employees 7%
- Expense reimbursement: <100 employees 17%, 100+ employees 13%
- Stimming: <100 employees 12%, 100+ employees 5%
- Cash on hand: <100 employees 8%, 100+ employees 16%
- Noncash: <100 employees 5%, 100+ employees 23%
- Financial statement fraud: <100 employees 5%, 100+ employees 5%
- Cash lacony: <100 employees 5%, 100+ employees 24%
- Payroll: <100 employees 2%, 100+ employees 6%
- Other: <100 employees 2%, 100+ employees 5%
THE RED FLAGS OF FRAUD

Understanding and recognizing the behavioral red flags displayed by fraud perpetrators can help organizations detect fraud and mitigate losses.

In 85% of cases, fraudsters displayed at least one behavioral red flag, and in 50% of cases, they exhibited multiple red flags.

These 6 behavioral red flags have been the most common in every one of our studies dating back to 2008, with a remarkably consistent distribution.

---

Red flags varied by perpetrator’s position:
- Unusually close association with vendor/customer: 24%
- Control issues, unwillingness to share duties: 21%
- "Wheeler-dealer" attitude: 22%
- Irritability, suspiciousness, or defensiveness: 18%
- Financial difficulties: 23%
- Complained about inadequate pay: 4%

Red flags varied by perpetrator’s gender:
- Financial difficulties: 39%
- Divorce/family problems: 20%
- Instability in life circumstances: 6%
- Unusually close association with vendor/customer: 11%
- "Wheeler-dealer" attitude: 6%
- Excessive pressure from within the organization: 3%
KEY FINDINGS – from the 2018 “REPORT TO THE NATIONS:

- 2,690 real cases of occupational fraud
- 125 countries
- 23 industry categories
- $7BILLION in total losses
- $130,000 median loss per cases
- 22% of cases caused Losses of $1million+
- Median duration of a fraud scheme – 16 months
- TIPS are by far the most common initial detection method
- Organizations with HOTLINES detect fraud by tips more often – 46%
- Organizations without HOTLINES – 30% of cases detected by tips

- Small businesses lost almost twice as much per fraud
  - Median loss for businesses with 100+ employees ----- $104,000.00
  - Median loss for businesses with <100 employees -------- $200,000.00
Criminals can easily capture your credit and debit card information with small devices called skimmers and their even more insidious cousins, shimmers. Don't fall victim to these sneaky attacks!

Instead of skimmers, which sit on top of the magstripe readers, shimmers are inside the card readers. These are very, very thin devices and cannot be seen from the outside. When you slide your card in, the shimmer reads the data from the chip on your card, much the same way a skimmer reads the data on your card's magstripe.

There are a few key differences, however. For one, the integrated security that comes with EMV means that attackers can only get the same information they would from a skimmer. On his blog, security researcher Brian Krebs explains that "data collected by shimmers cannot be used to fabricate a chip-based card, but it could be used to clone a magnetic stripe card. Although the data that is typically stored on a card's magnetic stripe is replicated inside the chip on chip-enabled cards, the chip contains an additional security components not found on a magnetic stripe."

The real problem is that shimmers are much harder to spot because they sit inside ATMs or point of sale machines. The shimmer shown in the article was found in Canada and reported to the RCMP. It's little more than an integrated circuit printed on a thin plastic sheet. If the owners of the compromised device hadn't been careful, this could have stolen the information from everyone who used it.
What is an Affinity Fraud?

Affinity fraud refers to investment scams that prey upon members of identifiable groups, such as religious or ethnic communities, the elderly, or professional groups. The fraudsters who promote affinity scams frequently are - or pretend to be - members of the group. They often enlist respected community or religious leaders from within the group to spread the word about the scheme by convincing those people that a fraudulent investment is legitimate and worthwhile. Many times, those leaders become unwitting victims of the fraudster's ruse.

These scams exploit the trust and friendship that exist in groups of people who have something in common. Because of the tight-knit structure of many groups, it can be difficult for regulators or law enforcement officials to detect an affinity scam. Victims often fail to notify authorities or pursue their legal remedies and instead try to work things out within the group. This is particularly true where the fraudsters have used respected community or religious leaders to convince others to join the investment.

Many affinity scams involve "Ponzi" or pyramid schemes, where new investor money is used to make payments to earlier investors to give the false illusion that the investment is successful. This ploy is used to trick new investors to invest in the scheme and to lull existing investors into believing their investments are safe and secure. In reality, the fraudster almost always steals investor money for personal use. Both types of schemes depend on an unending supply of new investors - when the inevitable occurs, and the supply of investors dries up, the whole scheme collapses and investors discover that most or all of their money is gone.
How To Avoid Affinity Fraud (U.S. Securities and Exchange Commission)

Investing always involves some degree of risk. You can minimize your risk of investing unwisely by asking questions and getting the facts about any investment before you buy. To avoid affinity and other scams, you should:

- Check out everything - no matter how trustworthy the person seems who brings the investment opportunity to your attention.
- Do not fall for investments that promise spectacular profits or "guaranteed" returns.
- Be skeptical of any investment opportunity that is not in writing.
- Don't be pressured or rushed into buying an investment before you have a chance to think about - or investigate - the "opportunity."
- Fraudsters are increasingly using the Internet to target particular groups through e-mail spams.
- Call the Texas State Securities Board 512-305-8300 in Austin.
Report identity theft and get a recovery plan.....

IdentityTheft.gov can help you report and recover from identity theft.

Here's how it works:

Tell us what happened.
We'll ask some questions about your situation. Tell us as much as you can.

Get a recovery plan.
We'll use that info to create a personal recovery plan.

Put your plan into action.
If you create an account, we'll walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.

**************************************************************************
IdentityTheft.gov is the federal government’s one-stop resource for identity theft victims. The site provides streamlined checklists and sample letters to guide you through the recovery process.

Visit ftc.gov/idtheft for prevention tips and free resources to share in your community.

Get your free credit bureau reports from.....“annualcreditreport.com”
**Does your company keep sensitive data — Social Security numbers, credit reports, account numbers, health records, or business secrets? If so, then you’ve probably instituted safeguards to protect that information. Your information security plans also should cover the digital copiers your company uses. If the data on your copiers gets into the wrong hands, it could lead to fraud and identity theft.**

**Digital Copiers are Computers**

Today’s generation of networked multifunction devices — known as “digital copiers” — are “smart” machines that are used for more than just copying; they can do everything from copying, printing, scanning, faxing to emailing documents. Digital copiers require hard disk drives to manage incoming jobs and workloads, and to increase the speed of production.

The hard drive in a digital copier stores data about the documents it copies, prints, scans, faxes or emails. If you don’t take steps to protect that data, it can be stolen from the hard drive, either by remote access or by extracting the data once the drive has been removed.
Before you acquire a copier:

Make sure it’s included in your organization’s information security policies. Copiers should be managed and maintained by your organization’s IT staff. Employees who have expertise and responsibility for securing your computers and servers also should have responsibility for securing data stored on your digital copiers.

When you buy or lease a digital copier:

Evaluate your options for securing the data on the device. Most manufacturers offer data security features with their digital copiers, either as standard equipment or as optional add-on kits. Typically, these features involve encryption and overwriting.

Encryption scrambles the data on the hard drive so it can be read only by particular software. Digital copiers that offer encryption encode the data stored on the hard drive so that it cannot be retrieved even if the hard drive is removed from the machine.

Overwriting — also known as file wiping or shredding — changes the values of the bits on the disk that make up a file by overwriting existing data with random characters. By overwriting the disk space that the file occupied, its traces are removed, and the file can’t be reconstructed as easily.
Common Personal Things to Remember:

- Your automobile is not a mobile file cabinet...if the bad guy can put your car up on 4 cinder blocks and remove all four wheels, your transmission, and your battery in 45 seconds how long do you think it takes them to remove personal information from your car.

- Ladies – your purse should never be left in your car...you may think it is well hidden, but the bad guys are watching and they are well aware that we are creatures of habit. Guys...the same goes for you...never leave your wallet or checkbook in the glove box or stuck behind the visor of your car...the bad guy is well aware of where to look.

- If I steal your car I can sell it once to a chop-shop...if I steal your personal information out of the mailbox I can sell it a thousand times on the internet.

- Do not leave outgoing mail in the mailbox...the next hand going into your mailbox is not necessarily the mailman. Meth addicts and Meth dealers need fast cash and stealing outgoing mail is a great way to make that cash and they can sell it more than once.

- The “read out” on your land-line or your cell phone can be made to read anything the fraudster wants it to read....IRS, County Clerk’s Office, Your Bank, Your Credit Card Company, etc.

- IRS or any government or law enforcement agency is not going to call you and give you a heads up that there is a warrant out for your arrest...why would they tell you ahead of time....all you would need to do is leave. If you owe IRS they are going to send you a certified letter explaining what you owe, how much you owe in fees, and by when you need to send the money. And they WILL NOT ask you to send your owed money in the form of “green dot cards” from Walmart, or “ITune cards” NOR will they ask you to send the money to an individual...they will want you to send it to the IRS.
Resources / Relationships:

- ACFE.com (Association of Certified Fraud Examiners)
- DOB.Texas.gov (Texas Department of Banking)
- FBI.gov
- IC3.gov (Internet Crime Complaint Center)
- FTC.gov (Federal Trade Commission)
- IdentityTheft.gov (Report identity theft and get a recovery plan)
- PostalInspectors.uspis.gov
- TexasAttorneyGeneral.gov
- Texas.SSB.gov (Texas State Securities Board)
- USSS.gov (United States Secret Service)
- Other Financial Institutions and Law Enforcement (local, state, and federal)
- annualcreditreport.com (get a free copy of your credit reports once a year)
CISA CYBER RESOURCES
Cybersecurity Advisors (CSAs)

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation’s Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.
CSA Deployed Personnel - Region 6

* CSA Offices
Incident Reporting/Malware Analysis

24x7 contact number: 1-888-282-0870


- If there is a suspected or confirmed cyber attack or incident that:
- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

Advanced Malware Analysis Center:

- Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.
- Must be provided in password-protected zip files using password “infected”
- Web Submission: https://malware.us-cert.gov
CISA Contact Information

George W. Reeves
Cybersecurity Advisor, Region VI
TX, AR, LA, OK, NM
Cybersecurity & Infrastructure Security Agency
Email: george.reeves@hq.dhs.gov
Mobile: (281) 714-1259
What’s Current in Payment Fraud
November 7, 2019

Questions???

Sandy Sullivan, CFE
Senior Vice President | Fraud Management
Frost Bank
(210) 220-5935 work | ssullivan@frostbank.com