RED FLAGS & FRAUD

What to look for and how to prevent it

Bob Tenuta
McHenry County College

WHAT FRAUDS/THREATS EXIST

- Identity Theft
- Check Fraud
- Electronic
- Phishing emails
- ACH Fraud
- Internal
- Collusion

IDENTITY THEFT

- Red Flag Rules
  - Section 114 of the Fair and Accurate Credit Transactions Act of 2003
- College is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:
  - Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
  - Detect Red Flags that have been incorporated into the Program;
  - Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
  - Ensure the Program is updated periodically to reflect changes in risks to students or college personnel or to the safety and soundness of the student or college personnel from Identity Theft.

RED FLAGS – KEY DEFINITIONS

- A "Covered Account" is any account the College offers or maintains that involves or is designed to permit multiple payments or transactions and any other account that the College offers or maintains for which there is a reasonably foreseeable risk to the customer or to the safety and soundness of the College from identity theft.
  - Based on current practices, the accounts referenced would include all student accounts, academic or financial, or accounts established through extensions of credit that are administered by the College.
- "Identifying Information" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including:
  - name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

RED FLAGS

- Suspicious Documents
- Suspicious Personal Identifying Information
- Suspicious Covered Account Activity or Unusual Use of Account
- Notifications and Warnings From Credit Reporting Agencies
- Alerts from Others
- Your own experience and observations

SUSPICIOUS DOCUMENTS

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address on an application is the same as the address provided on a fraudulent application;
  - The phone number on an application is the same as the number provided on a fraudulent application.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
  - The address on an application is fictitious, a mail drop, or prison;
  - The phone number is invalid, or is associated with a pager or answering service.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

- The SSN provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

- Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
  - The address does not match any address in the consumer report;
  - The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
  - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

SUSPICIOUS COVERED ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

- For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
- The financial institution or creditor is notified that the customer is not receiving paper account statements.
- The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

NOTIFICATIONS AND WARNINGS FROM CREDIT REPORTING AGENCIES

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of the interagency guidelines.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
  - A recent and significant increase in the volume of inquiries;
  - An unusual number of recently established credit relationships;
  - A material change in the use of credit, especially with respect to recently established credit relationships; or
  - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

SUSPICIOUS COVERED ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

- Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
  - The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
  - The customer fails to make the first payment or makes an initial payment but no subsequent payments.

SUSPICIOUS COVERED ACCOUNT ACTIVITY OR UNUSUAL USE OF ACCOUNT

- A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example
  - Nonpayment when there is no history of late or missed payments
  - A material increase in the use of available credit;
  - A material change in purchasing or spending patterns;
  - A material change in electronic fund transfer patterns in connection with a deposit account; or
  - A material change in telephone call patterns in connection with a cellular phone account.

ALERTS FROM OTHERS

- The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

DETECT RED FLAGS

- Obtaining Identifying Information and Verifying Identity
- Authenticating Transactions for Existing Customers
- Monitoring Transactions (Activity) Of Customers
- Verifying the Validity of Change of Address

PREVENTION & MITIGATION

- Continue to monitor a Covered Account for evidence of Identity Theft;
- Contact the student or college personnel as applicable per situation;
- Reset any passwords or other security devices that permit access to Covered Accounts;
- Provide the student or college personnel with a new student or college personnel identification number in person with proper identification;
- Notify the Program Administrator for determination of the appropriate step(s) to take;
- Notify law enforcement;
- File or assist in filing a Suspicious Activities Report; or
- Determine that no response is warranted under the particular circumstances

PROTECTING PERSONNEL IDENTIFYING INFORMATION

- Ensure that the College's website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing student or college personnel account information when a decision has been made to no longer maintain such information, subject to applicable document retention laws and policies;
- Ensure that office computers with access to Covered Account information are password protected;
- Avoid use of social security numbers;
- Ensure computer virus protection is up to date; and
- Require and keep only the kinds of student or college personnel information that are necessary for College purposes.

CHECK FRAUD

- Online Spending, Selling, and Renting
  - Many websites allow you to purchase items if you provide your bank's name and routing number along with your account number and billing address. Not all sites guarantee that they verify the true identity of customers' accounts, so someone with your checking information could make fraudulent purchases.
- Account Takeover
  - Account takeover happens when a thief gets your financial information and changes your mailing address to one he can access. This way, he can empty your bank account before you even realize a cent is missing.
- Paperhanging
  - Many types of inks are easy to remove from checks, which enables a thief to delete the name of the payee and write in a new name and a different amount. If you can't prove you didn't write the stolen check, you might be held liable for it.

CHECK FRAUDS

- Check Washing
  - Many types of inks are easy to remove from checks, which enables a thief to delete the name of the payee and write in a new name and a different amount. If you can't prove you didn't write the stolen check, you might be held liable for it.
- Check Kiting
  - Check kiting happens when a thief opens accounts at two or more banks to create fraudulent balances and take advantage of the time it takes for checks to clear. Check kiting results in the false inflation of an account balance, which allows checks that wouldn't otherwise clear to do so.
  - For example, a criminal might deposit a check for $100 in one account, then write a check from that account for $300 and deposit it into a second checking account. Before the bank can process the first deposit, the criminal immediately withdraws $300 in cash from the second checking account.
- Counterfeiting and Check Alteration
  - Counterfeiting a check can be done in two ways: A thief fabricates a check with special publishing equipment or duplicates a check using a state-of-the-art photocopier. Check alteration happens when a thief uses chemicals to break down the writing on a check and alters the information on it, similar to check washing.

CHECK FRAUD

- Forgery
  - Businesses are the most common victims of forgery. For example, an employee will take a check from his employer, write himself a sum of money, and cash it using his own ID or a fake ID and credentials.
- Fake Paychecks
  - If someone recruits you or you see a job posting online for a work-from-home or telecommute role, make sure it is legitimate. Some scams present this type of job with an offer of a first paycheck or bonus check in advance before you've done any work.
  - In this scam, the fraudster will either try to obtain your bank account information or will send you a fake check asking you to cash it or deposit and withdraw it, keeping a portion for yourself and wiring a portion back to them.

HOW TO IDENTIFY FRAUDULENT CHECKS

- The check lacks rough edges or perforations.
- Your name is printed in a different font from your address or other information on the check.
- The address of the bank or the customer is missing.
- You see a shiny, magnetic ink character recognition code at the bottom of the check. Real MICR ink is dull, so a shiny, glossy appearance often indicates a counterfeit check.
- The check has stains or discolorations, possibly from a thief using altering chemicals.
- Missing security padlock icon 

INFORMATION TO VERIFY

Information to Verify	Description
Bank Contact Information	Verify the bank name, bank address and phone number, especially if it is from a foreign bank.
Payor and Payee Contact Information	Check that any names are printed correctly and that the signature is or at least appears genuine.
Bank Account Numbers	You, your bank or the issuing bank can verify that the bank's routing number and the payee's account number are correct.
Date and Amount	Make sure the date and amount of the check are correct, particularly that the amount is not for more than what is due.
Overall Accuracy	Any misspellings, typos or other inconsistencies can be signs of fraud.

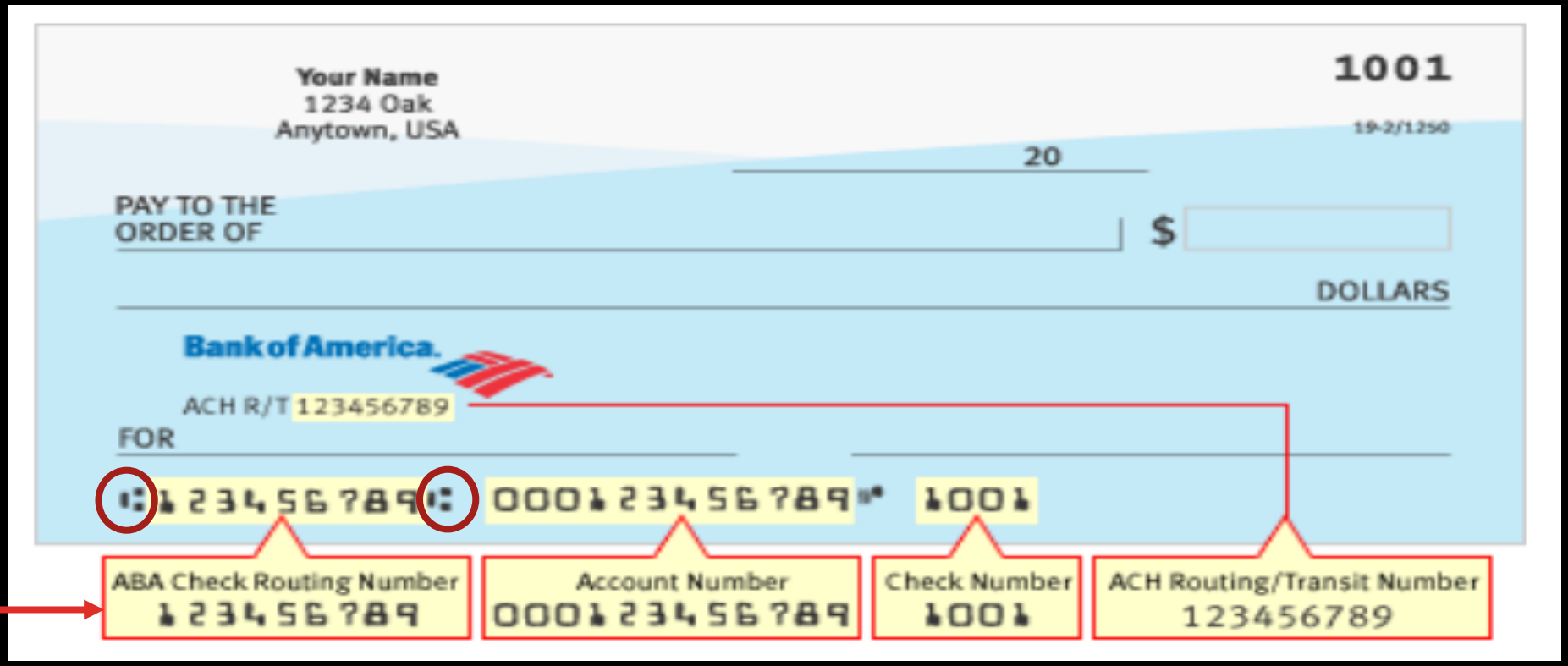
ROUTING NUMBER AND THE FIRST TWO NUMBERS ON A MICR LINE

Federal Reserve Banks

Federal Reserve Districts

Location	Banks	CU & Thrifts
Boston	01	21
New York	02	22
Philadelphia	03	23
Cleveland	04	24
Richmond	05	25
Atlanta	06	26
Chicago	07	27
St. Louis	08	28
Minneapolis	09	29
Kansas City	10	30
Dallas	11	31
San Francisco	12	32

MICR LINE



ABA/Routing # always a 9 digit number

Magnetic Ink Character Recognition

HOW TO PROTECT YOURSELF AGAINST CHECK SCAMS

- Write checks only to trustworthy individuals and companies;
- Mail your checks in a secure manner or deliver them in person;
- Use a gel pen to prevent check washing;
- Balance your checkbook every month without fail. Many people fail to open their bank statements every month, which is risky because you might be the victim of check fraud and not even know it;
- Cut down on the number of checks you're writing. Writing a check to pay your credit card bill is one thing; writing a check to pay the cashier for your weekly groceries might can be riskier;

ELECTRONIC FRAUD

- Computer and Network Intrusions
  - Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the country.
  - Who is behind such attacks?
    - from computer geeks for bragging rights to businesses hacking competitor websites for advantage, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes
- Ransomware
  - Hospitals, school districts, state and local governments, law enforcement agencies, small businesses, large businesses—these are just some of the entities impacted by ransomware, an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.
  - Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam e-mails, but because e-mail systems got better at filtering out spam, cyber criminals turned to spear phishing e-mails targeting specific individuals.
  - In newer instances of ransomware, some cyber criminals aren't using e-mails at all—they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

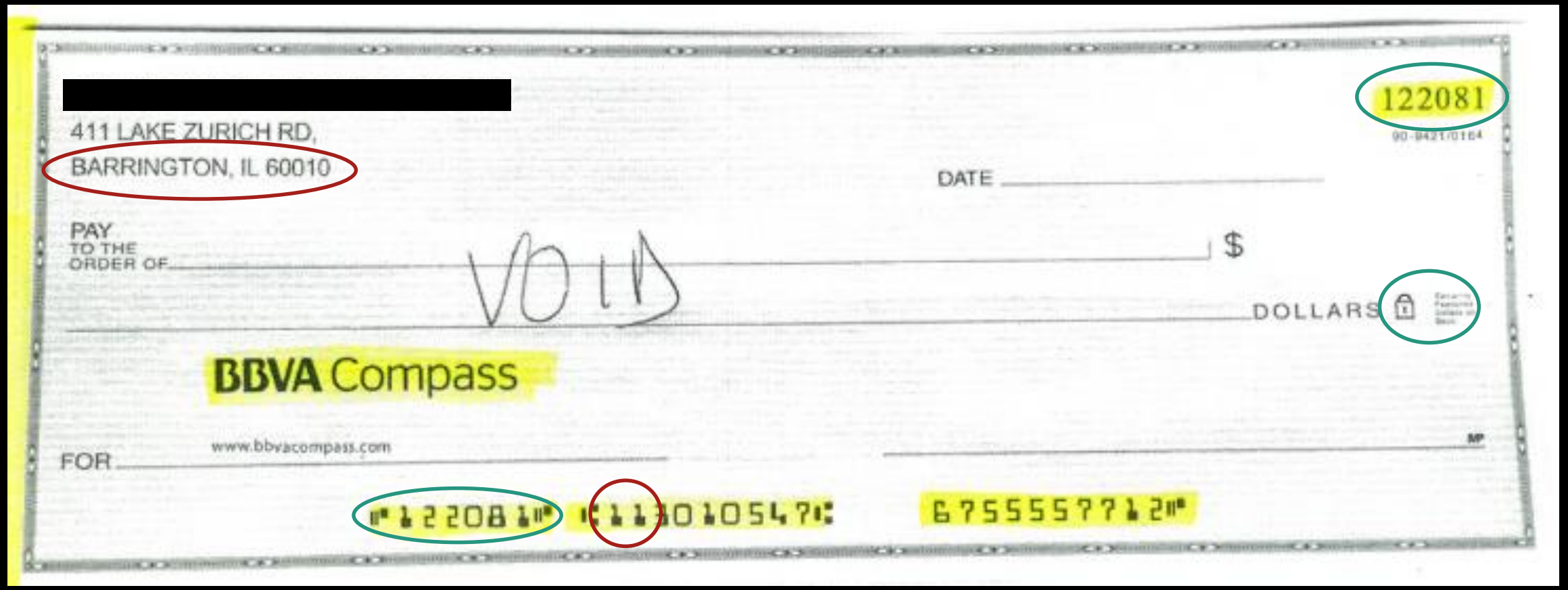
DEALING WITH RANSOMWARE

- Make sure employees are aware of ransomware and of their critical roles in protecting the organization's data.
- Patch operating system, software, and firmware on digital devices (which may be made easier through a centralized patch management system).
- Ensure antivirus and anti-malware solutions are set to automatically update and conduct regular scans.
- Manage the use of privileged accounts—no users should be assigned administrative access unless absolutely needed, and only use administrator accounts when necessary.
- Configure access controls, including file, directory, and network share permissions appropriately. If users only need read specific information, they don't need write-access to those files or directories.
- Disable macro scripts from office files transmitted over e-mail.
- Implement software restriction policies or other controls to prevent programs from executing from common ransomware locations (e.g., temporary folders supporting popular Internet browsers, compression/decompression programs).
- Back up data regularly and verify the integrity of those backups regularly.
- Secure your backups. Make sure they aren't connected to the computers and networks they are backing up.

ACH FRAUD

- The criminal accesses a commercial customer's credentials, generates an ACH file in the originator's name, and quickly withdraws funds before the victim discovers the fraud.
- The criminal accesses a retail customer's credentials and sets himself up as an automatic bill pay recipient.
- In an insider threat scenario, an employee of the target company or a bank modifies ACH files to steal money.
- In a variation on check kiting - a scam in which funds are juggled back and forth between bank accounts at separate banks - a criminal takes advantage of the time lag in transactions.
- In a spear phishing scam, an employee with authorization for ACH transactions receives an email that leads him to an infected site, which installs a keylogger to access authentication information. The thief can then impersonate the company's authorized representative and withdraw funds.

REAL, FAKE, OR FRAUD?



PHISHING

- Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
  - The word "phishing" is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim.
- Three types
  - Phishing;
  - Spear Phishing; and
  - Whale Phishing

EMAIL PHISHING

- For what purpose?
  - Hijack your usernames and passwords;
  - Steal your money and open credit card and bank accounts in your name;
  - Request new account Personal Identification Numbers (PINs) or additional credit cards;
  - Make purchases;
  - Add themselves or an alias that they control as an authorized user so it's easier to use your credit;
  - Obtain cash advances;
  - Use and abuse your Social Security number;
  - Sell your information to other parties who will use it for illicit or illegal purposes;

SPEAR PHISHING - DEFINED

- Spear phishing is an email-spoofing attack that targets a specific organization or individual, seeking unauthorized access to sensitive information.
- Spear-phishing attempts are not typically initiated by random hackers, but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.
- Spear phishing has the same goal as normal phishing, but the attacker first gathers information about the intended target. This information is used to personalize the spear-phishing attack. Instead of sending the phishing emails to a large group of people, the attacker targets a select group or an individual. By limiting the targets, it's easier to include personal information -- like the target's first name or job title -- and make the malicious emails seem more trustworthy.
- Whale phishing is highly targeted to individual C-Level managers.

PHISHING - HOW DO I KNOW?

- Requests for confidential information via email or instant message;
- Emotional language using scare tactics or urgent requests to respond;
- Misspelled URLs, spelling mistakes or the use of sub-domains;
  - www.barclays.com.142.ru vs. www.barclays.com
  - Subdomain tutorial
    - https://youtu.be/sDmErvLJSnc
- Links within the body of a message;
- Lack of a personal greeting or customized information within a message. Legitimate emails from banks and credit card companies will often include partial account numbers, user name or password.

EXAMPLE: 4-1-9 (A.K.A. NIGERIAN BANK SCAM)

Article 419 of the Nigerian Criminal Code deals with obtaining property by false promises, which is exactly what the advance-fee fraud is all about

REQUEST FOR URGENT BUSINESS RELATIONSHIP

FIRST, I MUST SOLICIT YOUR STRICTEST CONFIDENCE IN THIS TRANSACTION. THIS IS BY VIRTUE OF ITS NATURE AS BEING UTTERLY CONFIDENTIAL AND 'TOP SECRET'. I AM SURE AND HAVE CONFIDENCE OF YOUR ABILITY AND RELIABILITY TO PROSECUTE A TRANSACTION OF THIS GREAT MAGNITUDE INVOLVING A PENDING TRANSACTION REQUIRING MAXIIMUM CONFIDENCE.

WE ARE TOP OFFICIAL OF THE FEDERAL GOVERNMENT CONTRACT REVIEW PANEL WHO ARE INTERESTED IN IMPORATION OF GOODS INTO OUR COUNTRY WITH FUNDS WHICH ARE PRESENTLY TRAPPED IN NIGERIA. IN ORDER TO COMMENCE THIS BUSINESS WE SOLICIT YOUR ASSISTANCE TO ENABLE US TRANSFER INTO YOUR ACCOUNT THE SAID TRAPPED FUNDS.

THE SOURCE OF THIS FUND IS AS FOLLOWS; DURING THE LAST MILITARY REGIME HERE IN NIGERIA, THE GOVERNMENT OFFICIALS SET UP COMPANIES AND AWARDED THEMSELVES CONTRACTS WHICH WERE GROSSLY OVER-INVOICED IN VARIOUS MINISTRIES. THE PRESENT CIVILIAN GOVERNMENT SET UP A CONTRACT REVIEW PANEL AND WE HAVE IDENTIFIED A LOT OF INFLATED CONTRACT FUNDS WHICH ARE PRESENTLY FLOATING IN THE CENTRAL BANK OF NIGERIA READY FOR PAYMENT.

HOWEVER, BY VIRTUE OF OUR POSITION AS CIVIL SERVANTS AND MEMBERS OF THIS PANEL, WE CANNOT ACQUIRE THIS MONEY IN OUR NAMES. I HAVE THEREFORE, BEEN DELEGATED AS A MATTER OF TRUST BY MY COLLEAGUES OF THE PANEL TO LOOK FOR AN OVERSEAS PARTNER INTO WHOSE ACCOUNT WE WOULD TRANSFER THE SUM OF US$21,320,000.00 (TWENTY ONE MILLION, THREE HUNDRED AND TWENTY THOUSAND U.S DOLLARS). HENCE WE ARE WRITING YOU THIS LETTER. WE HAVE AGREED TO SHARE THE MONEY THUS; 1. 20% FOR THE ACCOUNT OWNER 2. 70% FOR US (THE OFFICIALS) 3. 10% TO BE USED IN SETTLING TAXATION AND ALL LOCAL AND FOREIGN EXPENSES. IT IS FROM THE 70% THAT WE WISH TO COMMENCE THE IMPORTATION BUSINESS.

PLEASE,NOTE THAT THIS TRANSACTION IS 100% SAFE AND WE HOPE TO COMMENCE THE TRANSFER LATEST SEVEN (7) BANKING DAYS FROM THE DATE OF THE RECEIPT OF THE FOLLOWING INFORMATIOM BY TEL/FAX; 234-1-7740449, YOUR COMPANY'S SIGNED, AND STAMPED LETTERHEAD PAPER THE ABOVE INFORMATION WILL ENABLE US WRITE LETTERS OF CLAIM AND JOB DESCRIPTION RESPECTIVELY. THIS WAY WE WILL USE YOUR COMPANY'S NAME TO APPLY FOR PAYMENT AND RE-AWARD THE CONTRACT IN YOUR COMPANY'S NAME.

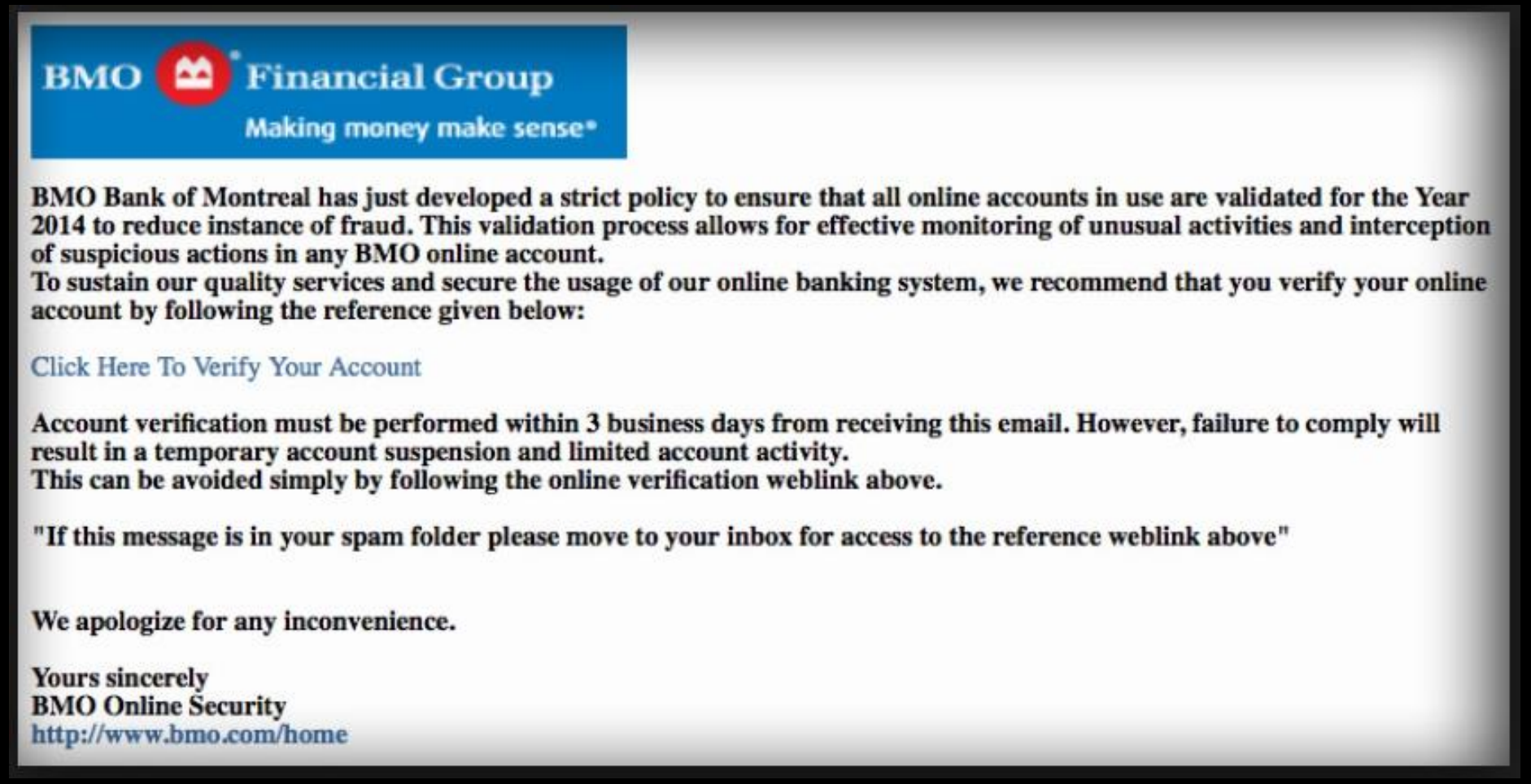
WE ARE LOOKING FORWARD TO DOING THIS BUSINESS WITH YOU AND SOLICIT YOUR CONFIDENTIALITY IN THIS TRANSATION. PLEASE ACKNOWLEDGE THE RECEIPT OF THIS LETTER USING THE ABOVE TEL/FAX NUMBERS. I WILL SEND YOU DETAILED INFORMATION OF THIS PENDING PROJECT WHEN I HAVE HEARD FROM YOU.

YOURS FAITHFULLY,

DR CLEMENT OKON

NOTE; PLEASE QUOTE THIS REFERENCE NUMBER (VE/S/09/99) IN ALL YOUR RESPONSES.

EXAMPLE: ACTIVE LINK SCAM



BMO Financial Group

Making money make sense®

BMO Bank of Montreal has just developed a strict policy to ensure that all online accounts in use are validated for the Year 2014 to reduce instance of fraud. This validation process allows for effective monitoring of unusual activities and interception of suspicious actions in any BMO online account.
To sustain our quality services and secure the usage of our online banking system, we recommend that you verify your online account by following the reference given below:

Click Here To Verify Your Account

Account verification must be performed within 3 business days from receiving this email. However, failure to comply will result in a temporary account suspension and limited account activity.
This can be avoided simply by following the online verification weblink above.

"If this message is in your spam folder please move to your inbox for access to the reference weblink above"

We apologize for any inconvenience.

Yours sincerely
BMO Online Security
http://www.bmo.com/home

EXAMPLE: ACTIVE LINK SCAM

- Legitimate website is www.gordonelectricsupply.com with locations in Kankakee Il. and Mokena Il.
- Actual email ext for this company is "@gordonelec.com"
- Criminal setup a domain email with "@gordonelectric.com"
- **WITHOUT CLICKING** **m**ouse over the link to reveal URL.
- Source in Ireland with a ".ie" extension
- Metadata in email finds IP 5.188.64.31, tracing it back to Kazakhstan.
- Alert your IT department
- Delete this email

EXAMPLE: USE OF LANGUAGE

From: Brandeis University <secure@brandeis.edu>
Date: Wed, Nov 13, 2013 at 7:13 AM
Subject: Confirm Your Brandeis University Account
To: Recipients <secure@brandeis.edu>

There is no "secure@brandeis.edu"

Dear User,

"Dear User" is common in phishing emails

We noticed irregular activity on your webmail account, and we have your account limited from sending email.

Follow our secure site link below to restore full webmail access.

https://www.brandeis.edu <http://z3ka.com/agcgitel/login.brandeis.edu.htm>

z3ka.com?

We apologise for any inconvenience

Yours Sincerely,

Brandeis University Services

There is no unit entitled "Brandeis University Services"

EXAMPLE: FOLLOW THE BAD LINK

Note the ".in" extension, it is originating out of India

FAKE EMAIL

From: Accounts | Pepper Construction [mailto:accounts@pepperconstructiongc.com]
Sent: Thursday, January 25, 2018 12:07 PM
To: Payables <payables@mchenry.edu>
Subject: ACH Form

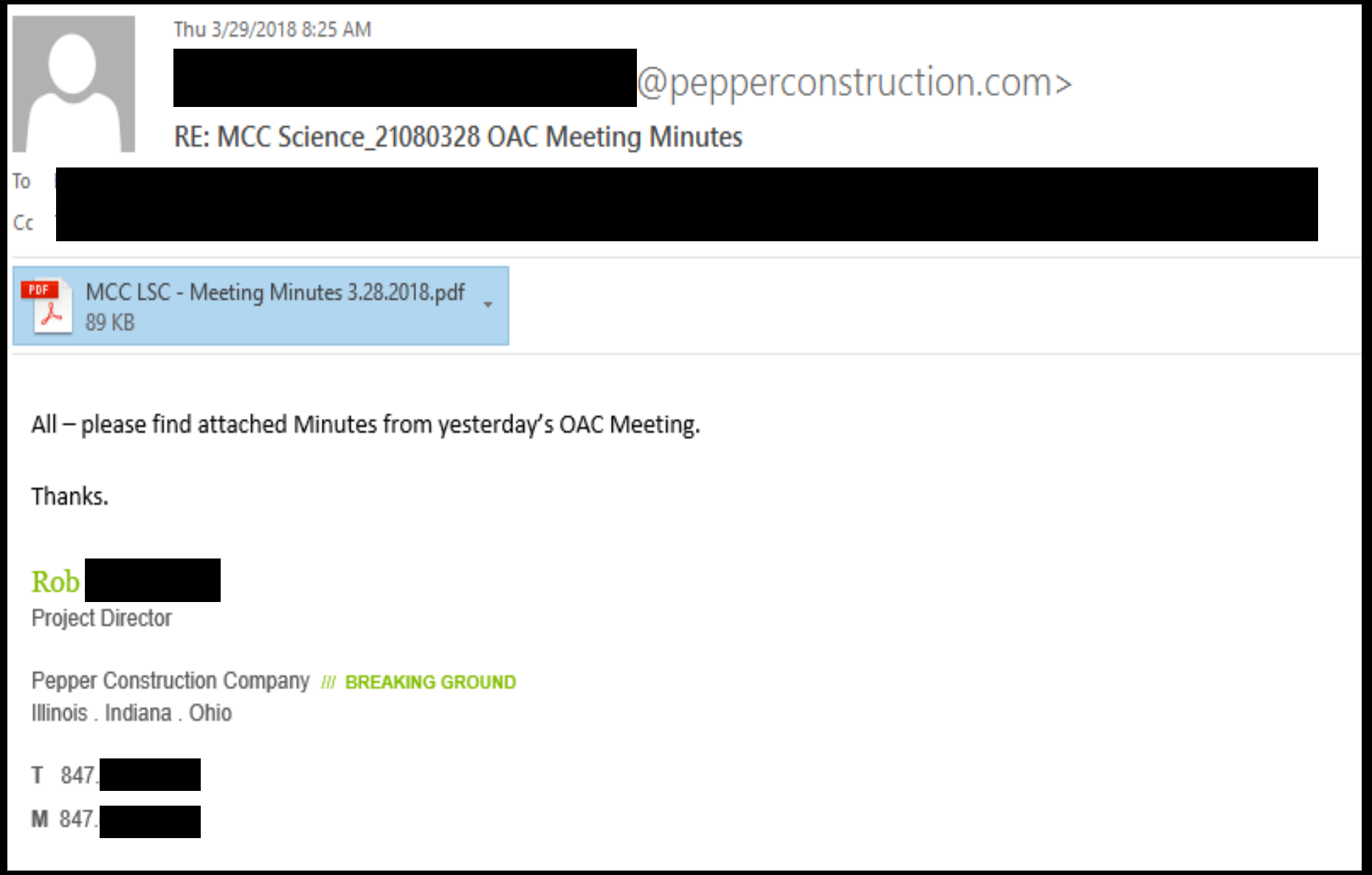
Can you kindly send us your ACH/Direct deposit form please?

Kind Regards,

Fiona Johnson | Accountant II | Finance Department
Tel: (847) 381-2760
Email: accounts@pepperconstructiongc.com

Pepper Construction

COMPANY'S REAL EMAIL



Thu 3/29/2018 8:25 AM

[redacted]@pepperconstruction.com>

RE: MCC Science_21080328 OAC Meeting Minutes

To [redacted]

Cc [redacted]

MCC LSC - Meeting Minutes 3.28.2018.pdf
89 KB

All – please find attached Minutes from yesterday's OAC Meeting.

Thanks.

Rob [redacted]
Project Director

Pepper Construction Company /// BREAKING GROUND
Illinois . Indiana . Ohio

T 847.[redacted]

M 847.[redacted]

PHISHING – PROTECTION?

- Do not provide personal information to any unsolicited requests for information
- Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser
- **If you suspect you've received phishing bait, contact the company that is the subject of the email by phone (to the contact on the vendor file of record) to check that the message is legitimate**
- Type in a trusted URL for a company's site into the address bar of your browser to bypass the link in a suspected phishing message
- Use varied and complex passwords for all your accounts
- Continually check the accuracy of personal accounts and deal with any discrepancies right away
- Avoid questionable Web sites
- Practice safe email protocol:
  - Don't open messages from unknown senders
  - Immediately delete messages you suspect to be spam

INTERNAL FRAUD

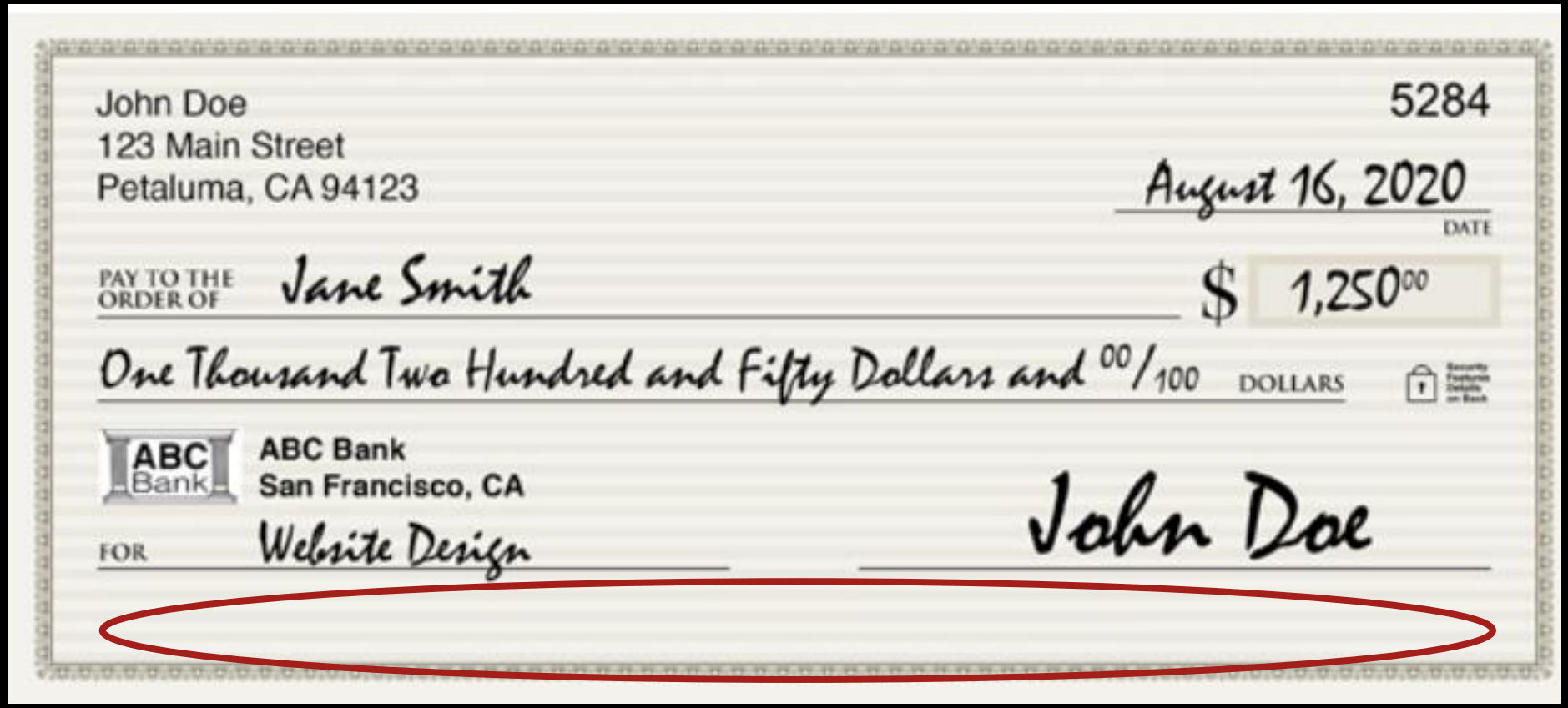
- Occurs when a member of staff dishonestly makes false representation, or wrongfully fails to disclose information, or abuses a position of trust for personal gain, or causes loss to others.
- Internal fraud can range from compromising customer or payroll data to inflating expenses to straightforward theft.
- Having sound internal controls help to deter fraud and detect it by having checks and balances in place.

COLLUSION

- Where two persons (or business entities through their officers or other employees) enter into a deceitful agreement, usually secret, to defraud and/or gain an unfair advantage over a third party, competitors, employers, consumers or those with whom they are negotiating.
- Collusion can include secret price or wage fixing, secret rebates, or pretending to be independent of each other when actually conspiring together for their joint ends.
- It can range from small-town shopkeepers or heirs to a grandma's estate, to gigantic electronics companies or big league baseball team owners.
- Very difficult to detect when employees collude.

QUESTIONS?

CHECK #1

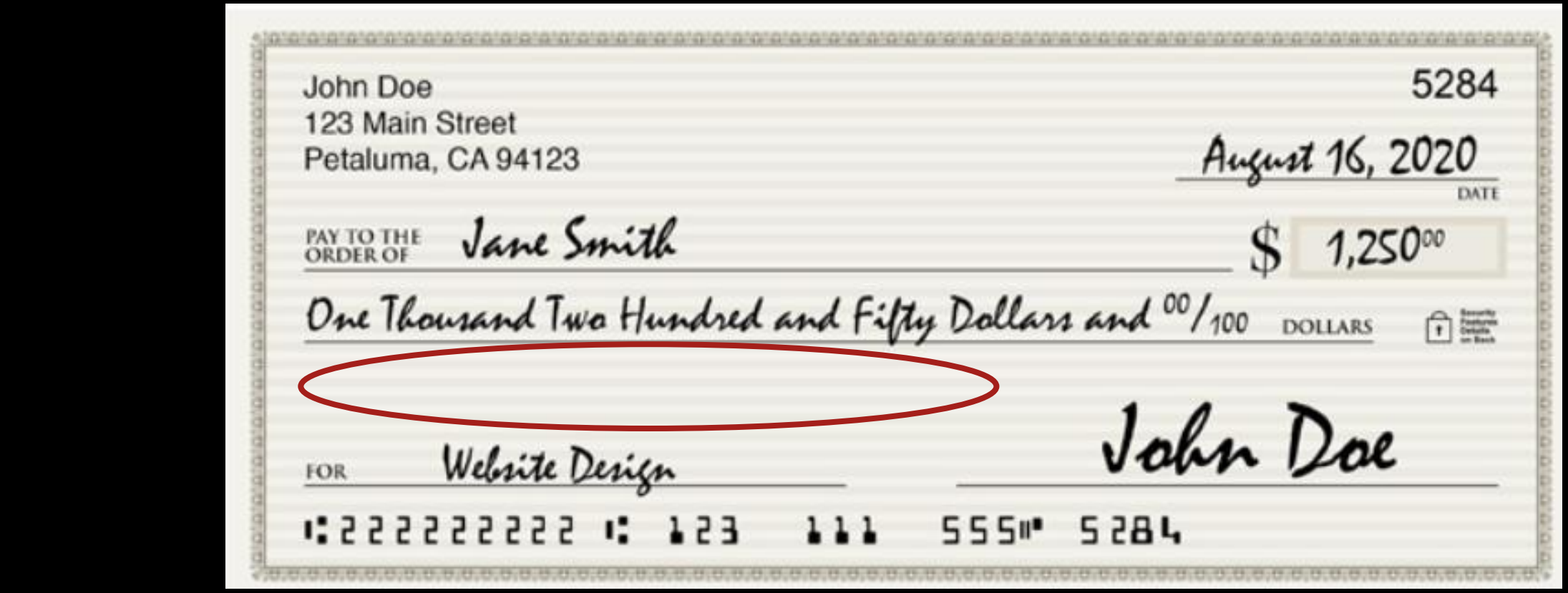


Check #1 - No MICR line

CHECK #2

Check #2 - Check #'s in upper right hand corner and MICR line don't match

CHECK #3

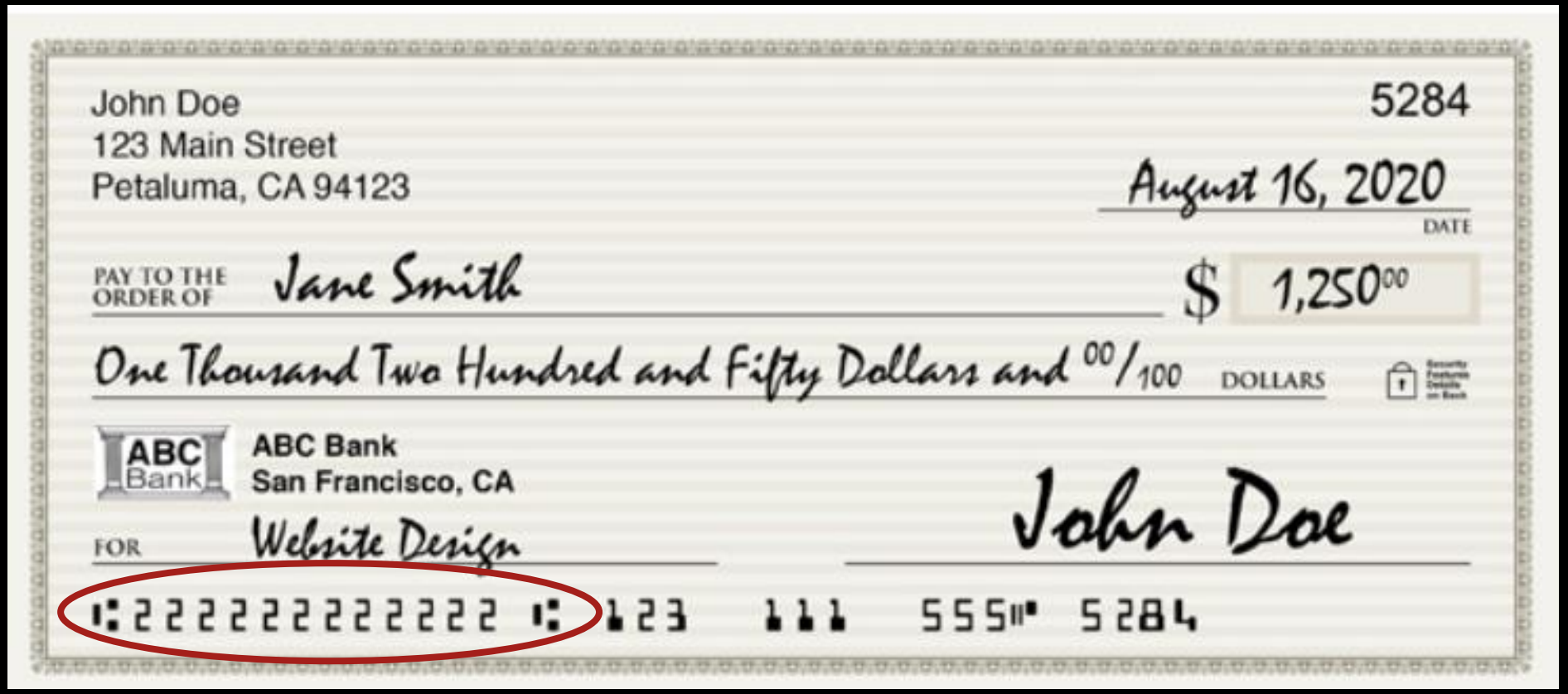


Check #3 - No bank logo or address

CHECK #4

Check #4 - Written and numeric dollar values don't match

CHECK #5

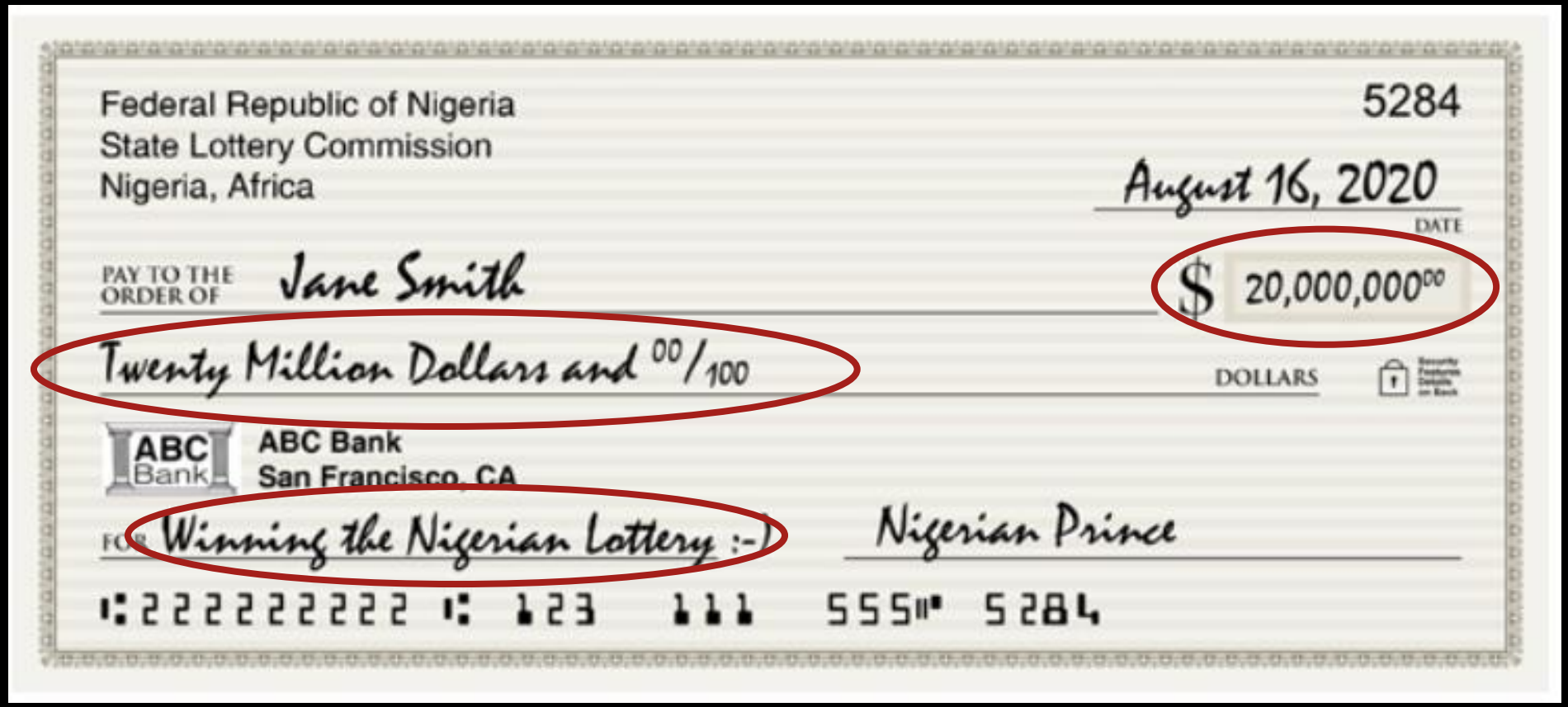


Check #5 - 12 digits in the routing #, routing #'s are always 9 digits long

CHECK #6

Check #6 - Account and signature names do not match

CHECK #7


Federal Republic of Nigeria
State Lottery Commission
Nigeria, Africa

5284

August 16, 2020
DATE

PAY TO THE ORDER OF Jane Smith

$ 20,000,000.00

Twenty Million Dollars and 00/100 DOLLARS

ABC Bank
San Francisco, CA

FOR Winning the Nigerian Lottery :-)

Nigerian Prince

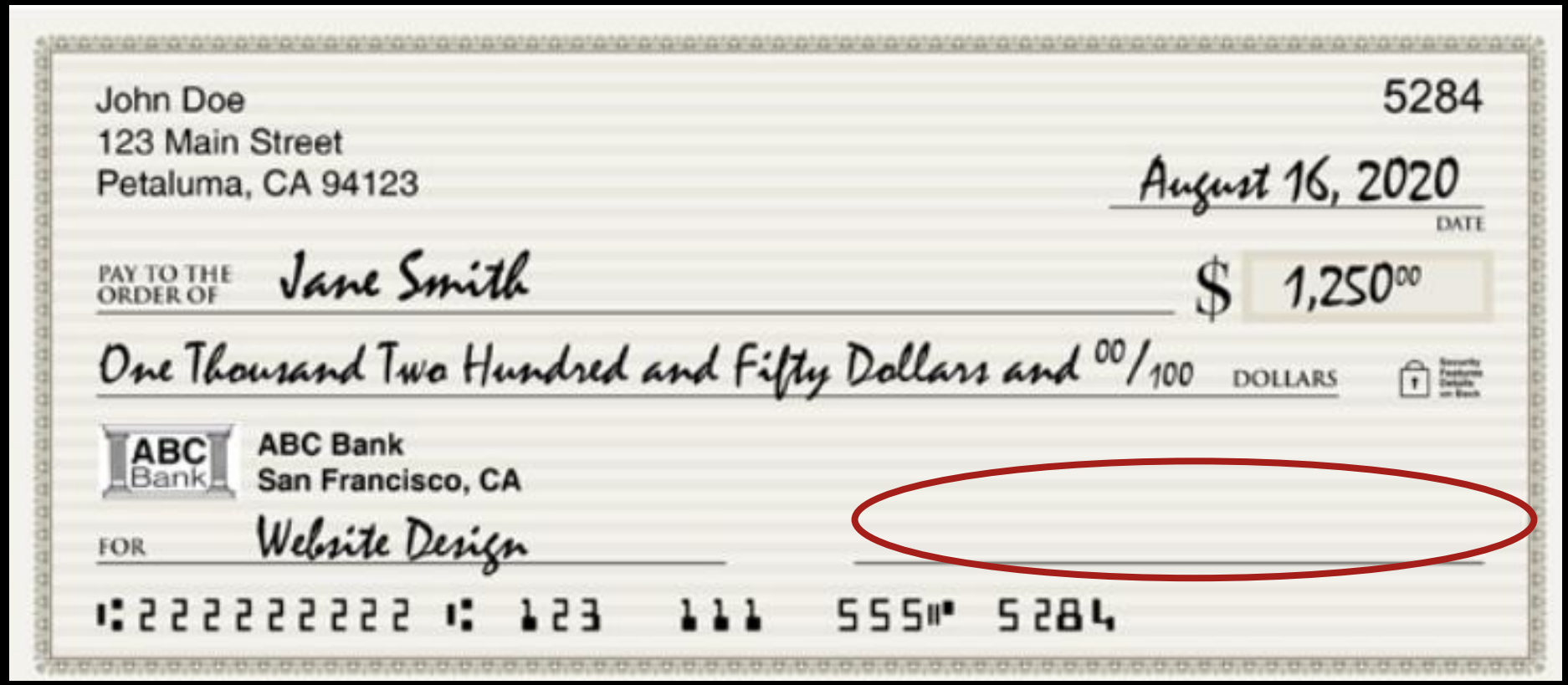
⑆222222222⑆ 123 111 555⑈ 5284

Check #7 - Unexpected source for outrageous amount

CHECK #8

Check #8 - No security padlock icon and right at the limit that raises suspicion

CHECK #9



Check #9 - Not signed

CHECK #10

Check #10 - This check is not fake, and will have a perforated edge after being torn from the register, which nearly all legitimate checks have.

CHECK TEST ANSWERS

- Check #1 - No MICR line
- Check #2 - Check #'s in upper right hand corner and MICR line don't match
- Check #3 - No bank logo or address
- Check #4 - Written and numeric dollar values don't match
- Check #5 - 12 digits in the routing #, routing #'s are always 9 digits long
- Check #6 - Account and signature names do not match
- Check #7 - Unexpected source for outrageous amount
- Check #8 - No security padlock and right at the limit that raises suspicion
- Check #9 - Not signed
- Check #10 - This check is not fake, and will have a perforated edge after being torn from the register, which nearly all legitimate checks have.