INDUSTRIAL BANK
Getting Things Done.

Empowering Our Community

Digital Defense - Safety and Security Best Practices

Safeguarding Your Bank Accounts

Top 5 Best Practices

Presented by: Jocelyn I. Boyd
VP/Deposit Operations Manager
Industrial Bank

Fraud Fighting Partnership

CONSUMER

FINANCIAL INSTITUTION

INDUSTRIAL BANK
Getting Things Done.

#1

Review Your Account Activity Regularly

- Online Banking
- Mobile Banking
- Telephone Banking
- E-Statements
- Paper Statements

INDUSTRIAL BANK
Getting Things Done.

#2

Safeguard Access To Your Account

- Password
- PIN Number
- Answers to Security Questions
- Account Number
- Checks

INDUSTRIAL BANK
Getting Things Done.

#3

Make Use of Account Alerts

SECURITY
Get alerts if someone changes your information or is trying to get access to your online banking.

BALANCE
Low balance alerts can help you avoid overdrafts or maintain balances to qualify for rewards. High balance alerts can help you identify when you might want to transfer or invest money.

TRANSACTION
Get alerts when deposits, checks, or withdrawals post to your account.

TRANSFERS
Get alerts when large incoming or outgoing transfers post to your account.

ATM/DEBIT CARD
Get alerts when ATM/Debit card transactions and changes occur.

OTHER
Get alerts when something unexpected happens.

INDUSTRIAL BANK
Getting Things Done.

#4

Consider Your Surroundings When Accessing Your Account

- ATM
- Gas Station
- Public Places
- Avoid Public Wi-Fi When Accessing Sensitive Data

INDUSTRIAL BANK
Getting Things Done.

#5

Beware Of Scammers and Unsolicited Calls or Email

- If it sounds too good to be true, it probably is.
- Contact your FI Immediately
- CFPB Consumer Education
- Federal Trade Commission
- Local Police or Sheriff's Office
- State Attorney General

INDUSTRIAL BANK
Getting Things Done.

Safeguarding Your Bank Accounts

Top 5 Best Practices

#1 Review Your Account Activity Regularly

#2 Safeguard Access To Your Account

#3 Make Use of Account Alerts

#4 Consider Your Surroundings When Accessing Your Account

#5 Beware Of Scammers and Unsolicited Calls or Email

INDUSTRIAL BANK
Getting Things Done.

INDUSTRIAL BANK
Getting Things Done.

For more information, please contact

Jocelyn I. Boyd
VP/Deposit Operations Manager
202-722-2000 Ext 3311
jboyd@industrial-bank.com

Safeguarding Your Bank Accounts

Jocelyn I. Boyd

Good evening and thank you for attending Industrial Bank's first session as we help to Empower Our Community. Continuing with the theme of the evening - **Digital Defense - Safety and Security Best Practices**, I'm going to focus on **Safeguarding Your Bank Accounts**. We will cover 5 best practices that based upon my experience in Banking Operations, based upon the types of calls we receive in Client Services, that these 5 recommendations are crucial to safeguarding your accounts. These recommendations are all free of charge and take very little time and effort to do. Feel free to share this information with your family and friends.

As a consumer, you have a responsibility to take steps to ensure the safety of your accounts. Although financial institutions invest in systems to detect account irregularities and to keep your accounts safe, you must play your part in the fight against fraud and account takeover. It's a partnership between you and your FI to fight fraud. Think about it, who would know better than you who the intended payee was on a check that you wrote? Who would know better than you if you authorized a recurring monthly debit to your account to pay a gym membership? What about the debit card that you misplaced but didn't report it to your financial institution because you figured you would find it eventually? It's in the house. Right? These are things that **only you would know** and if any unauthorized activity results from any of these things, you would be the **first to know**. So, it's important that you take action to alert your financial institution immediately if something is questionable. Well, how can you do that? The 5 best practices that we are about to cover will put you in the position to detect when something isn't right so that you CAN alert your FI

Let's cover the 5 best practices to help to Safeguard Your Bank Accounts.

1. Review Your Account Activity Regularly

What do I mean by regularly? At a very minimum you should review your account monthly **however** it is strongly recommended that you review your account more frequently. Online Banking, Mobile Banking, and Telephone Banking all give you 24/7 access to your account information and are great tools to make use of. I

personally recommend the first two as they will allow you to see check images, if you write checks. Seeing the image of a check in many times is critical in detecting fraud. Remember when I asked who would know better than you who the intended payee was on a check that you wrote? That's where this comes into play.

Your FI also provides you with periodic statements, generally monthly statements. eStatements allow you quicker access to your periodic statement and can be accessed through online banking or sent to you by secure email. This is the preferred method for receiving your statement. We also provide paper statements via US Mail as an alternative however it's not preferred considering the timing and delays in receiving statements in the mail and also the potential a fraudster could have of intercepting the receipt of your statement in the mail before you retrieve it from your mailbox.

2. Safeguard Access to Your Account

Never share your password or pin number with anyone. Your FI will never ask you for that information. If you have a joint account, each account holder should have their own password for online access and their own pin number for their ATM or debit card. Don't use the same password for all systems you access. Don't use the last four digits of your SSN for the PIN. Make it difficult or close to impossible for someone to get access to your accounts. For mobile use, make sure you have a password on your phone for access.

Get creative with answers to your security questions. Keep in mind no one is testing you to see if the answers are correct. So if you are asked 'What's your favorite food? The answer doesn't have to 'pizza' even if it is. Maybe your answer is Chicago or New York. Get it?

Avoid questions and answers that someone could do a Google Search or Zabasearch to find the answers to like the Street you grew up on or Your mother's maiden name.

Safeguard your account number and also your checks. If providing your account number to someone, be sure you know who you're giving it to and how it will be used. Why is it needed? Make sure you use a secure portal of providing the account number. Remember, your account number is on a need-to-know basis

only. With your checks, avoid writing checks to someone who you don't know. For example, someone comes door to door in your neighborhood, unsolicited who is repairing or painting mailboxes and wants to know if you want yours painted for $20. You agree and when the job is finished you realize you don't have any cash. You ask if the person will accept a check and he says "yes, make it out to Joe Scammer". You give Mr. Scammer the check and you never see him again. But do you realize that you've give Mr. Scammer more than just a $20 check. You've given him your Name, Address, Name of Financial Institution, Routing Number, and Account Number. You've even given him your signature! I'm not saying that someone who is repairing mailboxes in your neighborhood is a scammer. What I am saying is that some or all of this information in the wrong hands could put your account at risk. Keep this in mind also for those of you who put your outgoing mail in your home mailbox for the mailman to take when he/she delivers your incoming mail. Fraudsters are known for taking mail from a mailbox. If you have outgoing mail to send, put it in an official postal mailbox, take it to the post office, or put it in the hands of the postal delivery person.

3. Make Use of Account Alerts

Alerts is a service provided by most FIs, generally free of charge, and accessible through online banking and mobile banking. This allows you to be notified when things that you deem out of the norm occur on your account. Here are examples of some of the categories in which certain events could trigger an alert to you. ONLINE BANKING PASSWORD WAS CHANGED – ACCOUNT BALANCE THRESHOLD FALLS ABOVE OR BELOW DESIGNATED AMOUNT - Withdrawal over threshold amount occurred – CARD TRANSACTION OVER THRESHOLD – OTHER – FEE ACCESSED OR CHARGEBACK ITEM. Make sure you take advantage of services such as Alerts that your FI offers.

4. Consider Your Surroundings When Accessing Your Account

When using an ATM, make sure you look around first. Is this in a safe area, well-lit area? At the ATM or the gas station – look for skimming devices on the ATM terminal or gas pump. Make sure no one is looking over your shoulder when entering your pin number. When in public places, be aware of your surroundings. Public places such as coffee shops, the library, your hotel, the airport, restaurants offer the use of free public Wi-Fi. Avoid using public WiFi when accessing

sensitive information such as your bank account or paying a bill. Keep in mind that free public Wi-Fi connections may not be secure. There are even some rogue Wi-Fi hotspots. You never know so the best practice would be just to avoid using public Wi-Fi so as not to jeopardize the confidentiality of your personal information If you do use public Wi-Fi, only browse websites that start with "https" When you're done browsing, be sure to log out of any services you were using.

5. Beware of Scammers and Unsolicited Calls

Beware of any emails or phone calls from numbers claiming to be your bank. If you're unsure, pick up the phone and call your bank to verify an email first. Don't call the number on the email. Look up the phone number for your bank and call that number.

Remember, if it sounds too good to be true, it probably is. If someone contacts you and offers you the deal of a lifetime where all you have to do is deposit this check for $10k into your account and wire $5k back to them while keeping the rest of the money for yourself. That's easy money for very little effort, right? . . . Don't do it!

Check out the Consumer Financial Protection Bureau (CFPB) website. There's a section under Consumer Education >Fraud & Scams that addresses all different types of scams . . . Charity Scams, Debt Settlement or Debt Relief Scams, Grandparent Scams, Foreclosure relief or mortgage loan modification scams, Imposter scams, mail fraud, money mule scam, mortgage closing scams, lottery or prize scams, romance scams, and wire transfer fraud.

You want to make sure that you report suspected or confirmed fraud on your account to your financial institution immediately.

Remember too, If you're a victim of a scam, you can report it to the authorities by:

- Submitting a complaint online with the Federal Trade Commission
- Contacting your local police or sheriff's office
- Reporting it to your state attorney general

So, to recap, I've given you 5 best practices for Safeguarding Your Bank Accounts. This by no means is a complete list however these recommendations take a very minimal amount of your time to follow but they are critical in the partnership with your FI in safeguarding your accounts.

Thank you so much for your time and attention this evening!