JONAH BANK OF WYOMING FIGHTING FRAUD

Jonah Bank of Wyoming

Building a Better Wyoming

Introduction

Whether it is school, work, or social events, many parts of our normal life have shifted from in-person to online. With these changes, unfortunately, also come malicious cyber-criminals looking to take advantage of this increase in on-line activity.

The security of your information and accounts is Jonah Bank's top priority. When it comes to protecting your accounts, we believe it is a joint effort on the part of Jonah Bank and all of our customers. To help you use the security built into our systems and to respond to any incident you may be involved in, we want to share with you a process based on the National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF) for protecting your accounts and fighting scammers.

We have taken the five core functions of Identify, Protect, Detect, Respond and Recover that make up the NIST framework and applied them to online banking and fighting fraud. These resources will give you the knowledge to be better equipped to identify scams and what to do if you do become a victim of fraud.

This guide serves as a supplement to the Jonah Bank Fight Fraud details on our website (https://www.jonah.bank/resources/educational-resources/fight-fraud). This guide contains several resources for helping you to identify your critical online financial accounts, who has access to them, the threats to them, how to protect them, how to monitor them and detect any incidents related to these accounts, and finally, how to respond and recover from any incidents.

We hope you find these resources valuable, and if you have any recommendations on how to improve upon these resources, please contact Jonah Bank.

Support

Should you require further assistance, please contact one of our customer service representatives:

Casper	Casper	Cheyenne	Cheyenne
777 West 1st St.	3730 East 2nd St.	205 Storey Blvd.	2015 Central Ave.
Casper, WY 82601	Casper, WY 82604	Cheyenne, WY 82009	Cheyenne, WY 82001
307-2374555	307-266-5662	307-773-7800	307-773-7850

Send us an email at Customer_Service@jonah.bank

JONAH BANK® OF WYOMING

JONAH BANK OF WYOMING FIGHTING FRAUD: IDENTIFY

Jonah Bank of Wyoming

Building a Better Wyoming

Identify Accounts and Risks

When it comes to your financial information and accounts, your first step in fighting fraud is to identify high value accounts, online services used to access those accounts, and systems that connect to these accounts. The second step is to record who has authorized access to these accounts, and what permissions they have been granted. The third step is to identify the threats and vulnerabilities to these accounts and services.

Institution	Account	Website	Users	Linked Services	Threats
Jonah Bank	Checking	www.jonah.bank	John Smith	Accounting Software	CATO, BEC

Support

Should you require further assistance, please contact one of our customer service representatives:

Casper
777 West 1st St.
Casper, WY 82601
307-2374555

Casper
3730 East 2nd St.
Casper, WY 82604
307-266-5662

Cheyenne
205 Storey Blvd.
Cheyenne, WY 82009
307-773-7800

Cheyenne
2015 Central Ave.
Cheyenne, WY 82001
307-773-7850

Send us an email at Customer_Service@jonah.bank

JONAH BANK® OF WYOMING

JONAH BANK OF WYOMING FIGHTING FRAUD: PROTECT

Jonah Bank of Wyoming

Building a Better Wyoming

Protect

Once you have identified your important accounts and the threats to them, it's time to put in place preventative controls to "Protect" them. Preventative controls for your online accounts focus on implementing safeguards to prevent or limit fraudulent activity. It involves the establishment of appropriate account controls, rights, approvals, alerts and card controls. This function aims to ensure the confidentiality, integrity, and availability of your accounts.
The below table is designed to help you visualize the controls you have put in place for each of your users, to better understand the risks each user presents, and the controls that could be added.

Customers can use this form to document the configured rights and permissions of all users within online banking. Documenting your permissions can help you determine if users have the correct set of rights and detect unauthorized changes to user permissions.

When completing the table on the next page, you can use the following key:

- **Site:** The site or service being protected.
- **User:** The user account/login ID you are documenting.
- **Security Settings:** List the security controls in place to protect the users login. This can include strong passwords, Multi-Factor Authentication (MFA), Secure Access Codes (SAC), the use of biometrics (Tough/Face ID).
- **Account Rights:** Account rights include which account the user has access to (you may need to use multiple rows), and whether the user has View, Deposit, and/or Withdrawal rights for the account.
- **Transaction rights:** Transaction rights include the types of transactions the user can perform from within online banking (Funds Transfer, Wire, ACH, Payroll), the right to draft, approve or cancel transactions, the requirement for Transaction Authorization codes, Dual Approval, and whether the user has access to view only their transactions or all transactions in the account.
- **Administrative Rights:** Administrative rights include the ability to manage subsidiaries, recipients, and users.
- **Feature Access:** Feature access includes any additional feature the user has access to, including Bill Pay, Positive Pay, and MRDC.

A more detailed Account Protections Control form is available at:
https://www.jonah.bank/sites/www.jonah.bank/files/jonahbankfightfraudprotect.xlsx

Example: Protective Controls Audit

Site	User	Security Settings	Account Rights	Transaction Rights	Administrative Rights	Feature Access
Jonah Bank	Jonah Smith	MFA, SAC, Touch ID	1101XXXX View, Deposit, Wthdraw	Funds Transfer, ACH	None	Bill Pay, MRDC

Support

Should you require further assistance, please contact one of our customer service representatives:

Casper
777 West 1st St.
Casper, WY 82601
307-2374555

Casper
3730 East 2nd St.
Casper, WY 82604
307-266-5662

Cheyenne
205 Storey Blvd.
Cheyenne, WY 82009
307-773-7800

Cheyenne
2015 Central Ave.
Cheyenne, WY 82001
307-773-7850

Send us an email at Customer_Service@jonah.bank

JONAH BANK® OF WYOMING

JONAH BANK OF WYOMING FIGHTING FRAUD: DETECT

Jonah Bank of Wyoming

Building a Better Wyoming

Detect

Detecting abnormalities within your accounts, or access to your accounts, can help stop fraudsters in their tracks and limit any malicious activity that may be occurring. When it comes to your online bank accounts, Jonah Bank has many tools in place to help spot, prevent, and alert on suspicious behavior before the fraudster has a chance to act.

Customers can use this form to document all the configured alerts for their accounts. Documenting your alerts can help you see where there may be a gap in your detective capabilities.

When completing the table on the next page, you can use the following key:

- **Alert Category**: The alert category is the system or source of the alert.
- **Alert Type**: The alert types can be grouped into Account, Transaction, Security, Administrative, and Feature.
- **Alert Settings**: Alert settings are the details of how the alert is to be triggered.
- **Destination:** The destination is how the alert is to be received (SMS, Voice, eMail, or Push), you could also include who the recipient of the alert is.

Support

Should you require further assistance, please contact one of our customer service representatives:

Casper	Casper	Cheyenne	Cheyenne
777 West 1st St.	3730 East 2nd St.	205 Storey Blvd.	2015 Central Ave.
Casper, WY 82601	Casper, WY 82604	Cheyenne, WY 82009	Cheyenne, WY 82001
307-2374555	307-266-5662	307-773-7800	307-773-7850

Send us an email at Customer_Service@jonah.bank

JONAH BANK® OF WYOMING

Example: Detective Alerts

Alert Category	Alert Type	Alert Settings	Destination
Online Banking	Transaction Alert	Alert for Every ACH Transaction	Email Accounting Team or Business Owner
Online Banking	Account Alert	Alert when my balance is below $1,500	SMS
Bill Pay	Security Alert	When the payee information is changed	SMS
Card Valet	Transaction Alert	Alert on All Transactions	Push Notification

JONAH BANK OF WYOMING FIGHTING FRAUD: RESPOND & RECOVER

Jonah Bank of Wyoming

Building a Better Wyoming

Incident Response & Recovery Procedures

When responding to an incident, having incident response forms ready to use will help you act quickly and document the incident. Prepared incident response forms can also help to ensure all aspects of an incident are addressed in an order designed to best respond to the incident.

Depending on the nature and scope of the incident, you may find having pre-created communication templates for customers and or the media to be of value.

To help with ensuring any incident response forms are completed accurately it would be beneficial to perform a table top exercise. A table top exercise is a simulated test of how you would respond to an incident should it occur. These are beneficial to familiarize staff with the incident response process as well as to identify any weaknesses that you could strengthen prior to strengthen your defenses.

The below Incident response template has been built specifically for the handling of an incident involving fraud on one of your accounts or cards. As the identification of fraud on an account is usually clear, the development of an incident response playbook to determine if fraud occurred is not necessary. Instead, it is more prudent to move immediately into responding to the incident.

Jonah Bank encourages you to create playbooks for other scenarios where an alert may not always mean an incident has occurred. More investigation through a series of questions (Plays) may be needed to determine if engaging in incident response is required. The creation of similar forms for the handling of other scenarios, including but not limited to, Business Email Compromise (BEC), Ransomware, physical destruction of premises, or other generic scenarios will help you respond to any incident.

Support

Should you require further assistance, please contact one of our customer service representatives:

Casper	Casper	Cheyenne	Cheyenne
777 West 1st St.	3730 East 2nd St.	205 Storey Blvd.	2015 Central Ave.
Casper, WY 82601	Casper, WY 82604	Cheyenne, WY 82009	Cheyenne, WY 82001
307-2374555	307-266-5662	307-773-7800	307-773-7850

Send us an email at Customer_Service@jonah.bank

JONAH BANK® OF WYOMING

INCIDENT RESPONSE TEMPLATE

Use this form to manage an incident involving fraudulent activity in one of your financial accounts.

Incident Details

Date and time of Incident:				
Name & Title of Person Reporting the Incident:				
Contact Information:	Ph:	Email:		
Type of Incident:	☐ACH ☐Check Fraud ☐Debit Card Fraud ☐Payroll ☐Bill Pay ☐ Identity Theft ☐ Credit Card Fraud ☐Wire Fraud			
Account Numbers:				
Amount:				
Recipient Details:	Routing Number:		Account Number:	
Users:	Names:		Login IDs:	
Transaction Authorization:	☐Physical Token ☐Virtual Token		Serial Number:	
For Check Fraud:	Check Number:		Check Amount:	
	Payee:		Memo:	
Fraud Channel:	☐Online Banking ☐Mobile App ☐Phone Scam ☐Phishing Scam ☐Business Email Compromise ☐Corporate Account Take Over			
Description:	*Provide a Description of the Incident*			

IMMEDIATE ACTIONS

☐Lock User Accounts ☐Enforce MFA ☐Review all Drafted/Approved/Processed Transactions
☐Review Permissions of Account ☐Change Users Password ☐Reset Password on Other Services/Accounts
☐If Administrative Account Compromised, Reset Passwords on all user accounts ☐Cancel Unauthorized Transactions
☐Initiate a Stop Payment on Fraudulent Checks ☐Call Jonah Bank

CONTACT JONAH BANK

Casper	307-237-4555			
Cheyenne	307-773-7800			
After Hours Debit Card	1-866-504-5111 (also contact Jonah Bank during normal business hours)			
After Hours Credit Card	1-844-546-8220 (also contact Jonah Bank during normal business hours)			
Details:	Contacted ☐	Employee Name:		
	Employee Phone:		Case Number:	

CONTACT LAW ENFORCEMENT

Casper Police:	307-235-8278 https://casperpolice.publicforms.us/sc/			
Cheyenne Police:	307-637-6525 https://www.cheyennepd.org/services/online-crime-reporting			
Internet Crime Complaint Center:	https://www.ic3.gov/Home/ComplaintChoice			
Details:	Contacted ☐	Date & Time:		
	Officer Name:		Officer Phone:	
	Case Number:			

ADDITIONAL CORRECTIVE ACTIONS				
Additional Actions * document these changes below	☐MFA on all High Risk Accounts ☐Close Impacted Accounts ☐Close Debit or Credit Cards ☐Implement Additional Card Controls* ☐Monitoring/Alert Changes *		☐Transaction Approval Changes * ☐Review SAC and TAC code delivery ☐Implement Check Positive Pay ☐Review All Users Permissions ☐Add Identity Theft Monitoring Services	
Other Actions & Details:				
Credit Freeze – Equifax:	Phone:	800-685-1111	Website:	https://www.equifax.com/personal/credit-report-services
Credit Freeze – Experian:	Phone:	888-397-3742	Website:	https://www.experian.com/help
Credit Freeze – TransUnion:	Phone:	888-909-8872	Website:	https://www.transunion.com/credit-help

RETURN TO NORMAL		
Payments Review:	Document what changes to your payment flow you will make to prevent the incident from reoccurring.	(Example – Dual Approval, Positive Pay)
Actions to Take to Retore Normal Operations	☐Re-enable any Disabled Accounts ☐Update User Permissions ☐Enroll New Cards in Card Valet ☐Update All Services Linked to Online Banking ☐Update Services With Your Account on File	Other Actions to Return to Normal:

DOCUMENTATION	
Documented Changes	*Document all implemented or planned changes to your payment flows or updates to user permissions and linked services.* (Example New Review Process for Confirming Payee Changes)

COMMUNICATIONS		
Messages to Be Communicated: Email, Phone, Mail	To Internal Stakeholders	Can be on the fly
	To Customers	A message template should be created
	To Media	A message template should be created

TEST & VALIDATE		
Control To Test:	Testing Scenario	Results of Test

POST INCIDENT REVIEW		
Lessons Learned:	Key Questions to Consider in the Post-Incident Review: • What were the root causes of the incident and any incident response issues? • Could the incident have been prevented? How? • What worked well in the response to the incident? • How can our response be improved for future incidents?	Answers/Details:
UPDATES TO POLICIES & PROCEDURES		
Policies and Procedures to Be Updated:		
Staff Training on New Policies and Procedures:		