NIST CSF 2.0 Core Functions Applied to Mitigate Financial Assets Vulnerable to Cyber Threat.

Asset	Identify	Protect	Detect	Respond	Recover	Govern
Customer Data	Classify and locate customer data; assess risks.	Encrypt data; restrict access to authorized personnel.	Monitor data access; detect unauthorized access.	Isolate affected systems; notify stakeholders; investigate.	Restore data from backups; improve protections; post-incident review.	Establish data governance policies; ensure regulatory compliance.
Network Systems	Map network architecture; identify critical components.	Implement firewalls, IDS/IPS, and network segmentation.	Deploy IDS; continuously monitor network traffic.	Isolate compromised systems; initiate incident response.	Restore network functionality; apply patches; post-incident analysis.	Implement network governance frameworks; align with organizational goals.
Employee Accounts	Inventory accounts; assess access levels and risks.	Enforce MFA; implement role-based access control.	Monitor account activity for anomalies; detect unusual behavior.	Disable compromised accounts; investigate; notify users.	Securely re-enable accounts; enhance security measures.	Develop account management policies; conduct regular reviews.
Financial Databases	Identify critical databases; assess security and compliance needs.	Encrypt data; apply strict access controls and audits.	Monitor database access; detect unauthorized queries.	Isolate affected databases; investigate; notify relevant parties.	Restore database integrity; enhance security; post-incident review.	Establish database governance; ensure regulatory compliance; regular reviews.
Online Banking	Identify key systems; assess operational and regulatory risks.	Use encryption; secure coding practices; regular security testing.	Monitor transactions; detect fraud and anomalies.	Suspend affected accounts; investigate; notify customers.	Restore services; communicate with customers; update security controls.	Implement governance for regulatory compliance and security best practices.
Mobile Banking Apps	Map app infrastructure; assess dependencies and risks.	Secure app development; encryption; regular security testing.	Monitor app usage; detect unusual behavior and malware.	Issue security updates; notify users; investigate root cause.	Restore functionality; issue patches; improve security practices.	Define secure development and compliance policies; regular reviews.

Cloud Storage	Identify data stored; assess security and compliance risks.	Encrypt data; enforce access controls; monitor access.	Monitor access logs; detect unauthorized access or data exfiltration.	Revoke unauthorized access; restore data; notify users.	Restore data access; review security protocols; post-incident analysis.	Develop cloud governance policies; align with objectives and compliance.
Third-Party Vendors	Identify vendors; assess risks and dependencies.	Enforce security agreements; conduct regular security audits.	Monitor vendor activities; detect deviations from normal behavior.	Work with vendors to contain issues; investigate; reassess vendor relationship.	Re-establish secure services; improve oversight; review vendor policies.	Implement vendor risk management policies; regular audits and reviews.
Encryption Keys	Identify all keys; assess storage and management practices.	Store keys securely (HSM/KMS); enforce access controls and key rotation.	Monitor key usage; detect unauthorized access or anomalies.	Revoke compromised keys; re-encrypt data; notify stakeholders.	Regenerate and securely distribute new keys; enhance key management practices.	Establish key management policies; align with industry standards; regular reviews.