SECURITY IDENTITY BREACH

Checklist

1	**Contact Your Financial Institutions**	**Bank and Credit Card Companies.** Freeze accounts and issue new cards. **Credit Reporting Agencies**. Equifax, Experian, and TransUnion - Place fraud alert or credit freeze.
2	**Review Your Credit Reports**	Obtain free copies of **credit reports** from AnnualCreditReport.com. Review unauthorized activity or accounts to dispute with credit bureaus.
3	**File a Report with the Federal Trade Commission (FTC)**	Go to **IdentityTheft.gov** to report theft. The FTC provides a recovery plan and you create an Identity Theft Report.
4	**Contact the Police**	File **police report** with local law enforcement. Helps provide evidences to creditors and other institutes.
5	**Update Your Passwords**	Changes **passwords and security questions** for all online accounts, social media and financial institutions. Use strong, unique passwords, and consider password manager.
6	**Monitor Your Accounts**	**Regularly** check bank statements, credit card and insurance statements for suspicious activity. Consider setting up alerts for unusual transactions.
7	**Notify the IRS (if necessary)**	If possible **Social Security Number Fraud,** contact IRS Identity Protection Specialized Unit and set up an Identity Protection PIN: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
8	**Place a Fraud Alert**	A **fraud alert** on your credit report warns creditors to take extra steps to verify your identity before opening new accounts in your name. Contact agencies listed in step 1.
9	**Consider Identity Theft Protection Service**	These services can **help monitor** your personal information and provide support in case of fraud.
10	**Keep Records**	**Document** all communications related to the breach, whom you contacted, dates, details of discussions. Helpful for creditors and law enforcement.