WHAT IS IT?
Financial abuse is behavior that seeks to control a person’s ability to acquire, use, or maintain economic resources, and threatens their self-sufficiency and financial autonomy(1).

WHY DOES IT MATTER?
99% of all survivors of domestic violence report experiencing some form of financial abuse(2).

If a survivor cannot afford to access and maintain safety, their choices are limited. They may be forced to remain with someone who is causing them harm, or depend on someone else for financial support. If they cannot maintain financial independence or access necessary resources, they may have to return to an abuser.

References
TECH SAFETY AND FINANCIAL ABUSE

Digital financial abuse can be perpetrated by misusing technologies such as online banking access, finance apps, or other tools to maintain power and control over survivors.

COMMON TYPES OF FINANCIAL TECHNOLOGY (FINTECH):
- Banking
- Payments
- Lending
- Investing
- Credit Monitoring
- Public Benefit Management

Fintech can be strategically used to easily access a variety of financial resources, and offers benefits such as:
+ Easy receipt of income
+ Remote access to funds and banking
+ Additional tools to monitor finances
+ Timesaving connections to banks, lenders, investment tools

This technology can also be misused as a tactic of abuse, particularly within intimate partner relationships. Abusers misuse fintech as a means of power and control by:
- Sending excessive, unprompted requests for funds
- Monitoring spending history through shared banking access
- Changing shared passwords to deny access to benefits
- Using online lenders to apply for credit in a survivor's name

STRATEGIES

10 Tips to Help Secure Your Financial Identity Information Online

1. Only share sensitive financial information with applications and organizations you trust.
2. Double-check the privacy settings of accounts and applications with sensitive personal information.
3. Review, secure, and/or remove publicly available information about you online.
4. Place spending alerts on credit cards and bank accounts.
5. Keep a budget and track monthly expenses.
6. Use a credit card or cash instead of a debit card for routine purchases.
7. Monitor your credit report and track any new inquiries or changes in your credit score.
8. Utilize fraud alerts for additional protection of your financial identity and credit.
9. Place a credit freeze on your credit report.
10. Use secure accounts, devices, and networks to access your financial accounts.
RECOMMENDATIONS

Beyond the steps that individuals can take to increase the safety of their financial identity information online, there are also ways that communities, businesses, and policymakers can support a safer financial landscape for survivors.

For Communities:
- Keep cash options available for consumers
- Partner with local DV programs for training on how tech is misused for financial abuse

For Financial and Tech Institutions:
- Financial institutions and fintech companies should screen for financial abuse
- Build capacity to voluntarily forgive coerced debt

For Policymakers:
- Require financial institutions to address and alleviate coerced debt
- Create public funding to address credit repair
- Fair financial regulation for the fintech sector

ADDITIONAL RESOURCES

- Safety Net Project
- TechSafety App
- Moving Ahead Curriculum
- Economic Justice Project
- Fintech: How Mobile Payment and the Gig Economy Can Help Enhance Survivor Safety (PDF)
- IdentityTheft.gov
- Security Planner

in partnership with NNEDV NATIONAL NETWORK TO END DOMESTIC VIOLENCE