Financial Abuse and Technology

What is Financial Abuse?

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]. For survivors of domestic violence, this may look like:

- Identity Theft: Impersonating an individual to gain access to existing accounts or open new ones.
- Controlling Funds: Monitoring an individual's spending or withholding their funds, either through direct access to the account or through other linked financial applications.
- Employment or Educational Sabotage: Preventing someone from securing or maintaining employment or educational opportunities.
- Ruining Credit: Taking out loans in someone's name, refusing to pay shared debts, or other actions resulting in negative impacts to credit.
- Coerced Financial Fraud: Forcing someone to file fraudulent tax returns, misuse benefits, or commit other financial crimes.

For more information about what financial abuse looks like, visit About Financial Abuse from the National Network to End Domestic Violence's (NNEDV) Economic Justice Project.

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.

[1] Adrienne E. Adams and Marisa L. Beeble, "Intimate Partner Violence and Psychological Well-being: Examining the Effect of Economic Abuse on Women's Quality of Life," Psychology of Violence 9, no. 5 (2019)

[2] Adrienne E. Adams, *Measuring the Effects of Domestic Violence on Women's Financial Well- Being* (Madison: University of Wisconsin-Madison Center for Financial Security, 2011)

Tech Safety and Financial Abuse

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

There are a variety of financial technology ("fintech") options available, offering different services and each with their own safety benefits and concerns.

Common types of fintech include online or app-based versions of financial services such as:

- Banking – allows you to access the traditional features of a bank, including checking and savings accounts, access to credit, etc.
- Payments – designed to facilitate exchanging money between individuals or payment to a retailer for goods and services.
- Lending – provides access to apply for and manage credit options, including making payments.
- Investing – tools for building an investment portfolio including stocks, bonds, high-yield savings, etc.
- Credit Monitoring – provides access to credit report, credit scores, and sometimes options for credit improvement.
- Public Benefit Management – online access to apply for benefits, monitor amounts and spending, provide income verification, etc.

Fintech can be strategically used to easily access a variety of financial resources, and offers benefits such as:

- Easy receipt of income. Survivors can access funds directly and more quickly than traditional methods, which can make all the difference when time is of the essence.
- Remote access to funds and banking. If a survivor has had to relocate for safety, it may be difficult to access a physical bank or in-network ATM. They may also struggle to get to a bank during typical business hours, and benefit from 24/7 access to accounts and mobile deposit features online.

- Additional tools to monitor finances. This can include online budgeting tools, access to bank and credit card statements, and methods for monitoring and securing their credit reports.
- Timesaving connections to banks, lenders, investment tools. Time is a limited resource, and safer, fast access to these resources can free up time to meet other needs.

Unfortunately, fintech can also be misused as a tactic of abuse, particularly within intimate relationships where an abuser may have increased access to information, devices, and accounts. Abusers misuse fintech as a means of power and control by:

- Sending excessive, unprompted requests for funds, which can be a drain on a survivor's time and resources, as well as causing stress.
- Monitoring spending history through shared banking access. Abusers may use this information to surveil a survivor and track where they have been making purchases.
- Changing shared passwords to deny access to benefits. Survivors who depend on access to government benefits (e.g., WIC, SNAP, or Medicaid), and who lose access to those benefits due to an abuser tampering with their accounts, may be forced to return to a dangerous situation in order to access food and healthcare.
- Using online lenders to apply for credit in a survivor's name. With access to information such as a survivor's legal name, date of birth, and social security number, an abuser may take out and use credit in a survivor's name, putting them into debt and making it more difficult for them to access the resources needed to leave.

Strategies

10 Tips to Help Secure Your Financial Identity Information Online

Online services have a lot of information about us! There are many digital tools available to manage your finances, and these tools all require some type of financial identity information, such as your name, social security number, credit score, or other personally identifying and sensitive information. It's important to ensure that your financial identity information is protected online to protect your accounts against unauthorized access.

When the person you are most concerned with protecting your finances from is a former intimate partner or someone who had access to your financial identity information, regaining control of your financial identity can feel very similar to being involved in a data breach. Below are 10 suggestions for how to secure your financial identity information online.

1. **Only share sensitive financial information with applications and organizations you trust.** Your data is a valuable commodity to many websites and applications (apps). Websites and apps will request sensitive information about your financial identity for a variety of purposes. Some will allow you to import banking information, such as the routing number and account number for your checking or savings accounts, for various purposes, such as payment processing, rental applications, and tracking expenditures. Sharing this information can help you achieve your financial goals more quickly, but it can also place your privacy at risk if the app or institution is not guarding your information adequately. Shared information can also pose a risk if an abuser has access to an account that is linked to information you don't want them to have, such as credit cards and banking information.

   When deciding which websites or apps to trust with your information, here are some essential questions to consider:

   a. Who is your information being shared with? Once you share your information with this institution or app, will it be shared with others? Can you choose who else this information is shared with? When evaluating the security and privacy of your accounts, it's important to learn if any account information or data may be shared with entities that you don't want to have access to it, such as third-party organizations. Consider this for both your bank and credit accounts and the apps you are sharing this information with. This information should be included in the privacy policy governing your account or application usage, but these documents are often

overlooked when opening a new account, or too long to read and understand in one sitting.

Banks, for example, have specific regulations around the information they can share with non-affiliated third parties. They can share information considered public (meaning it could be obtained from a public source, legally, even if the bank received the information directly from you) with companies outside the bank without offering customers an opt-out option. Banks can also share certain non-public personal information (including that you are a customer of the bank, purchases made with your credit card, and other personally identifiable financial information) with non-affiliated third parties. In general, the bank is required to allow you to opt-out of this sharing, though there are certain exceptions to the opt-out requirement[3]. For more information on how your financial identity information can be used by banks, visit the Federal Deposit Insurance Corporation's (FDIC) Privacy Rule Handbook. This rule only applies to banks, but other companies should still have a privacy policy you can review, and may offer opt-outs for certain information sharing.

b. How is your information being used? What is the purpose of collecting your information? Often financial institutions and fintech apps request or require access to your personal information to achieve their intended purpose. Before sharing, consider: is this information necessary for you to achieve your goals in using the app features or account services? If not, is there another way to achieve these goals without sharing this information? For example, could a potential landlord review paystubs or another form of income verification, rather than requesting sensitive banking information?

[3]FDIC. "Privacy Rule Handbook." FDIC.gov. Last modified 2023. https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/index.html.

c. What protections or measures are in place to ensure that your personal information is protected once it's entered into the application? If an app is requesting access to sensitive financial identity information, the app should be transparent about how your information is being used and protected. Make sure you are using the correct app for the financial institution or fintech application of your choice, and download it from a trusted app store. The Apple and Google app stores provide users with an overview of how each app handles data, written by the developer, that can be reviewed prior to downloading the app. You can also review user ratings to see if other customers have had security issues with the app. Additionally, some anti-virus programs like Norton 360 can help you determine whether an app is reputable or not, what information that app collects, and who that information is shared with. These programs can be a useful tool in determining whether an app meets your privacy needs, but they usually require a fee or paid subscription and may not be accessible to all survivors.

   Norton recently partnered with TechSoup in collaboration with NNEDV to donate product licenses for survivors recovering from financial and tech abuse. For more information on this partnership and how victim service programs can connect survivors with these products, visit the TechSoup blog.

2. **Double-check the privacy settings of accounts and applications with sensitive personal information.** If you are concerned about an unauthorized person gaining access to your account, consider increasing password security and implementing multi-factor authentication. Some financial apps have settings which share transaction history with the public or even with friends listed in your device's contacts. It may be difficult to hide the existence of these accounts from people looking for your presence on these apps, but there are steps you can take to increase your privacy. Avoid using

features like importing your contacts, which may connect you with people you do not want to have access to your personal information. In most cases, you can take steps to restrict their access to you on these apps (such as blocking). Make sure your settings protect information you do not want shared.

3. **Review, secure, and/or remove publicly available information about you online**. There are a range of ways to manage your digital fingerprint, some free and some requiring one-time payment or a monthly fee.

   Personally identifying information such as your name, address, email address, phone number, and other data may end-up online in a few different ways: you may share it voluntarily, someone else may share it on your behalf, it may be distributed by data brokers (whose role is to purchase, collect, and sell information from various sources), or it may be obtained in a data breach.

   A simple way to see what's publicly available about you online is by using a search engine to look-up your name and see what information appears in the results. This will primarily show information from the first three sources mentioned, as information released in a data breach is not typically easily accessed through online searches.

   a. If you come across information you previously shared that you wish to remove, you can manage or remove this yourself as long as you still have access to the account. If you no longer have access to the account, it may take additional steps to regain access to the account you shared the information from.
   b. If you see information someone else shared about you that you do not want shared, check out Safety Net's resource on removing sensitive information from the internet for more information.

c. If you see information gathered by data brokers, you have options to get it removed! Check out Safety Net's resource on data brokers for more information.

There are several free and paid options to determine if your information has been compromised in a data breach, and what information may be exposed. One such option is have i been pwned?, which will search known data breaches for your email address, and allows you to sign up to receive notifications of future breaches. Some services may conduct searches for additional sensitive information, such as usernames, passwords, SSN, or birth date. Once you're aware that your information has been involved in a data breach, it's important to update passwords to secure any current accounts, and not to reuse a leaked password for any other accounts.

4. **Place alerts on credit cards and bank accounts** so you are notified via text or email when a purchase is made, balances are low or high, a failed login attempt is made, or other changes are made to your accounts. These alerts may vary from account to account, but will generally allow you to choose which types of changes cause a notification so you can personalize them to meet your security needs. For transaction alerts, you can often set the level of expense that will trigger an alert, so you can check for small purchases or deposits (often used to test whether an account is active and see if anyone is monitoring it), or only be notified of larger expenses (if you are concerned an abuser may attempt to make large purchases or drain a shared account).

   Setting such alerts can notify you of unauthorized purchases or account access more quickly than other fraud detection services, which may require a more noticeable pattern or change to trigger an alert. Before setting up these types of alerts, make sure that you are not sending these notifications to a device or email address that is or could be monitored by the abusive person, as this could increase your safety risk.

5. Another way to monitor for unauthorized purchases is to **keep a budget and track monthly expenses**. You can keep a budget manually, or use budgeting tools to track your expenses. Some budgeting tools can be set up to import transaction data directly from accounts, making the process of tracking transactions quicker and more convenient, but ensure you only share this information with websites and apps you trust (see Tip #1). There are many additional benefits to keeping a budget, such as better knowledge of your overall financial health and the ability to identify spending patterns and ways to save. For more information on budgeting basics and under financial fundamentals, check out Module 2 of Allstate and NNEDV's Moving Ahead Curriculum.

6. If you have access to credit, one way to protect your finances is to **use a credit card instead of debit for routine purchases**. Ideally, use a credit card that has never been shared with the abusive person so that your purchases cannot be monitored. This can offer an additional level of protection above cash assets if a card is skimmed or card information is otherwise misused. Most credit and debit cards offer some level of protection against unauthorized purchases and will not hold the cardholder liable for fraudulent charges. Even so, it can often take time to dispute these charges and get them cleared from an account. Using a credit card will also protect cash assets against instant withdrawal. If you have multiple credit cards, using specific cards for specific types of purchases (e.g. groceries, gasoline, etc.) can help make fraud or other unauthorized spending easier to detect if it occurs.

   Note: This method requires access to credit, which is not accessible to all people who are looking to secure their financial identity. If you do not have access to credit, another method of protecting your banked funds is to pull out cash for transactions that you feel are high-risk or you do not want monitored.

7. **Monitor your credit report and track any new inquiries or changes in your credit score.** There are several free and paid

options for monitoring changes to your credit report. By visiting AnnualCreditReport.com, you can request a free copy of your credit report from each of the three nationwide consumer reporting agencies every 12 months. Some of the consumer reporting agencies will let you sign up for an account and receive additional copies of their report. It's important to note that credit reports will show active and closed credit accounts, how much debt you have, and payment history, they typically do not include a credit score. If you want to review your credit score, this article from the Consumer Financial Protection Bureau lists several ways to find out your credit scores. Credit scores are determined based on the information included in your credit reports, so if you find fraudulent activity or errors in your credit report, it can impact your credit score.

If you are looking for automated monitoring or more frequent reports, there are options available for paid services that can help you track your credit activity more closely.

8. **Utilize fraud alerts for additional protection of your financial identity and credit.** Fraud alerts notify potential creditors that you have been or may be a victim of fraud, and encourages them to take additional steps to verify your identity before extending a new line of credit. There are two types of fraud alerts: initial and extended. You can request an initial fraud alert for any reason, and it will remain on your credit report for one year. Initial fraud alerts can be renewed annually as needed. An extended fraud alert is only available to victims of fraud with certain types of documentation, such as a police report, FTC Identity Theft Report, or Affidavit of Fraud confirming fraud and/or identity theft. This type of fraud alert will remain on your credit report for up to seven years unless you opt out earlier and will stop you from receiving any pre-screened credit card and insurance offers for 5 years.

   Both types of fraud alerts will also allow you to request additional copies of your credit report free-of-charge for credit monitoring purposes. You only need to request a fraud alert through one of the

three nationwide credit bureaus (Experian, TransUnion and Equifax), who will then communicate with the other two on your behalf.

9. **Place a credit freeze on your credit report.** Anyone can request a credit freeze, but if you believe your financial identity information has been compromised, or if you have been the victim of fraud, it can be an important step to increase your security. A credit freeze restricts access to your credit report for the purposes of extending credit in your name. This can prevent someone from opening a credit account fraudulently with your name, even if they have information about your financial identity. You can unfreeze or "thaw" your credit when you need to allow a creditor access to your report, such as when applying for a credit card, renting an apartment, or buying a car.

   To freeze or thaw your credit, you must contact each credit bureau individually. You will be asked to verify your identity, and may need to provide documentation to do so. If you know which credit bureau(s) a potential creditor needs to access in order to approve an application, you can thaw your credit with only those bureaus, for the length of time required by the creditor, as an extra layer of security.

   The three national credit bureaus also offer a service called credit lock (which may be a free or paid service) which operates similarly to a credit freeze, but offers a faster method for freezing and thawing credit on demand. It's important to note that while the credit bureaus are required by law to offer credit freezes, credit locks are governed by the policies of the companies offering them, and may not offer the same legal protections as a credit freeze.

   If you are the victim of identity theft, you can visit IdentityTheft.gov to develop a personalized recovery plan based on your situation.

10. **Use secure accounts, devices, and networks to access your financial accounts.** Secure devices and networks help to ensure that accounts remain free from outside interference. A former partner may have information about you including your social security

number, date of birth, or other security question information that companies such as your bank or other financial institutions may typically use to authenticate your identity. If you have shared an account with someone in the past who you no longer trust, you may need to take certain steps to ensure that you are the only one with access now. If you added a former partner as an authorized user on a payment account, you may be able to revoke their access. If the account was opened jointly, you may need to close the account and open a new account to ensure they don't have access. Contact your credit card servicer or bank for more information and to determine your next steps.

Some financial institutions may sell your data to or share your data with third parties for marketing purposes. This may result in receiving unsolicited offers for credit and other contacts. If these unsolicited offers come to an email or mailing address that an abuser has access to, they could be alerted that you have opened a new account, or receive information including the amount of debt you currently hold.

One way to prevent unauthorized access is to secure personal accounts with a PIN or password only known to you. For additional information on information on securing accounts and devices, check out Safety's Net's guides on Securing Devices and Accounts and safer password management. Safety Net also has resources on increasing the security of your internet connection. If you're interested in increasing the overall security of your information online, Consumer Reports' Security Planner walks you through creating a free, custom security plan based on your devices and concerns.

Recommendations

Beyond the steps available to individual survivors to secure their financial identity information, there are ways that other societal actors can begin supporting survivors of financial abuse. Below are some recommendations for communities, financial institutions and tech companies, and

policymakers. These recommendations are only the beginning; they will not solve all of the ways in which systems currently disadvantage survivors. There is much more to be done to create social and financial systems which actively support survivors of abuse, but it's our hope that survivors, advocates, communities, financial institutions, tech companies, and policymakers can continue to work together to make meaningful change.

For Communities:

- **Keep cash options available for consumers.** Cash may be the only accessible means of payment for survivors fleeing financial abuse, and it has the benefit of not being easily tracked. When businesses transition to cashless payment systems, they remove options for those without the ability to safely use digital currency.
- **Partner with local DV programs for training on how technology is misused for financial abuse.** Informed communities can better support survivors of financial abuse and craft policies that all survivors to fully participate in local economies.

For Financial and Tech Institutions:

- **Financial institutions and fintech companies should screen for financial abuse** in the course of their daily operations. These institutions should include language within their reporting features that allow survivors to easily report incidents. Early detection means less potential for ongoing financial abuse, and can help survivors identify abuse and access resources sooner. This also means less financial harm that institutions must deal with later.
- **Institutions should build capacity to voluntarily forgive coerced debt**, enabling survivors to rebuild credit sooner and with less penalties for debt they did not willingly accrue.

For Policymakers:

- **Require financial institutions to address and alleviate coerced debt.**

- **Create public funding to address credit repair.** When survivors are not shouldering coerced debt and the burden of rebuilding credit following financial abuse, they are able to seek safety and focus on healing.
- **Fair financial regulations for the fintech sector** should include supports for survivors of violence and financial abuse.

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
- IdentityTheft.gov
- Security Planner

© 2024 National Network to End Domestic Violence, Safety Net Project.
The creation of this resource was made in partnership with Norton, part of the Gen family of brands. Opinions, findings, and conclusions or recommendations expressed in this guide are NNEDV's.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.