Identity Abuse: Identity Theft and Impersonation

Guilherme Roschke

Guilherme Roschke is a staff attorney at the ABA Commission on Domestic Violence where he provides technical assistance on electronic privacy and cyberlaw issues to domestic violence attorneys, as well working on the Commission's legal education programs. Prior to joining the Commission, Guilherme was a Skadden Fellow at the Electronic Privacy Information Center in Washington, DC. His fellowship focused on protecting the privacy of victims of domestic violence. Prior to law school Guilherme was a computer programmer with experience in corporate, non-profit and scientific environments. Guilherme is a member of the DC and NY bars. He received his JD from The George Washington University Law School.

Identity theft is defined generally as using another's personal information to impersonate them and therefore obtain something of value, collect more information on the victim, or otherwise harm the victim. Abusers can easily engage in identity theft because they often have access to the personal information of their victim. Identity abuse can cause harassment, frustration, safety risks and a negative economic impact, making it hard for a survivor to find a new lease, new employment or a new mortgage. Clearing these errors and frauds from a credit report can take substantial amounts of time.

The basic form of identity theft is "new account fraud." Using some of the victim's personal information, like a social security number and address, the perpetrator opens a new account in the name of the victim intending to gain some value in the process. For example, by getting a credit card in the name of another, the perpetrator can make purchases under the victim's name. Typically, this is hard for a victim to detect because the perpetrator is opening accounts with entities that the victim is unrelated to, and the notice of the new accounts is directed to the perpetrator, not the victim.

Another form of identity theft is "existing account fraud." This is the use of an existing account, such as a credit card, debit account or bank account to buy goods or services. Detecting this is easier because the victim already knows the account exists, gets regular updates on the account, and has a relationship with the account provider.

"Pretexting" is another form of identity theft, this one with potentially large safety risks. Generally the term refers to one person interacting with a third party under the "pretext" of being another person. Specifically, it has been used to refer to the practice of telephone pretexting, where one person is able to gain access to the telephone records of another. In response to this, the Federal Communications Commission issued new rules for phone companies to protect their customer records.[1] Congress also passed the Telephone Records and Privacy Protection Act of 2006, providing stiff penalties for purchasing, selling or transferring confidential telephone records information.[2] However, pretexting can be used in other contexts, such as to gain information directly from the victim, which can be used for further crimes. For example, Amy Boyer was shot and killed by a stalker that paid a pretexter for her employment location – the

company that provided the information to the stalker was later judged to be liable for turning over the information.[3]

Detecting Identity Theft: Get Credit Reports

Identity theft in the form of new account fraud can most readily be detected by checking a client's credit report. Checking the report will also aid the client in finding errors or other problems that may be a barrier to economic freedom, employment or renting. In addition, this process serves other privacy protection purposes, like showing the client and the lawyer the information that public records have about the client.

A credit report will contain several types of information. It will contain identification, payment history, inquiries and public record information. The identification will contain current and past addresses, employment, social security number, date of birth and any aliases – for example, a maiden name. Payment history will contain reported credit accounts such as credit cards, student loans, and telephone or other utility bills. Inquiries include a listing of times a credit report has been accessed by employers, creditors or others checking the report. Public record information will contain information such as bankruptcies, court judgments and tax liens. From this information the credit bureaus will also calculate a credit score. The credit score is made available to creditors requesting the report and can also be purchased by the individual that is the subject of the report.

Federal law provides that consumers may get free credit reports in several circumstances, but most importantly, are also entitled to one free report per year from each of the major credit bureaus.[4] This offer does not include the credit score, but these must by law be made available for purchase. The only website created for this purpose is http://www.annualcreditreport.com.[5] Consumers are also entitled to free reports when they are unemployed and seeking work, when they are on welfare, when they have reason to believe that fraud has occurred, or when they receive notice of an adverse effect on their credit.[6]

Correcting a Credit Report & Preventing Further Identity Theft

Once the credit report is obtained it should be read and scanned for errors or fraud. The report should come with information on how to correct it. One key document to be prepared is an "identity theft report." This will contain all the fraudulent accounts and evidence for the fraud, and must be filed with a law enforcement agency. Correcting your report will require you to submit copies of this, including proof of its filing, to the credit bureaus. Further information can also be found at the website of the Federal Trade Commission.[7] Victims should maintain a log of the effort required to correct the report, so that perpetrators can be held accountable.

State and Federal law and credit reporting agency practices provide two ways to help prevent further identity theft – placing a "fraud alert" on a credit report, or requesting a "credit freeze," sometimes called a "security freeze." One can place a 90 day fraud alert when they suspect their information could be used for identity theft, such as when a wallet is stolen or when they are about to serve a protection order on the abuser. A longer lasting seven year fraud alert can be placed once it is verified that identity theft has occurred. Doing this requires filing an identity theft report and submitting it to the credit bureaus. Fraud alerts warn creditors that there is potential fraud on the account. Creditors are to confirm the identity of the person seeking credit.

Fraud alerts do not prevent a credit report from being issued – so a stalker is still able to access a victim's credit report. However, a credit or a security freeze can prevent a credit report from being issued. This prevents identity theft because creditors will not issue new credit without a credit report. It also prevents stalkers from improperly accessing a credit report. The freeze can be selectively lifted temporarily or for particular creditors. Federal law does not guarantee credit freezes, but the main credit bureaus offer them for a fee. State law may allow free access to credit freezes for identity theft victims. Consumer's Union has a website that shows credit freeze laws state by state.[8] Proper planning is required for a successful use of credit freezes: many steps a survivor takes legitimately require credit lookups. A survivor should be aware that a new employer or new landlord may require the freeze to be lifted. Further, existing credit accounts will need exceptions to the freeze as well, since many creditors continuously check the credit scores of their debtors.

Online Impersonation: Non-Financial Identity Theft

Identity theft doesn't have to be financial in nature. One potential form of abuse is to impersonate the victim in a way to cause harassment, injury to reputation, or other harm. This can include sending emails or other communications in the name of the victim to third parties, or posting fake online profiles or personal ads. These can cause embarrassment, libel, third-party harassment, or interference with work. For example, in one case, a perpetrator in a same sex relationship posted a victim's pictures and work voice and fax number in a gay themed online hookup website. The victim was in the military and thus faced potential "don't ask don't tell" sanctions from the contacts the workplace received.

Identity theft laws may not cover this kind of impersonation, because the harm is not financial fraud. Harassment and/or stalking laws may provide better relief. However, in Wisconsin, a woman was recently charged under their identity theft statute for posting a fake online dating profile of her ex-partner.[9] The profile stated that the partner was gay and sought other men to contact him at his work address. The statute in question prohibits using the personally identifying information of an individual, without authorization, to "harm the reputation, property, person or estate of the individual."[10]

Addressing Identity Theft in a Civil Protection Order

If identity theft is suspected by a domestic violence, sexual assault or stalking client, a Civil Protection Order should seek to remedy it. Remedies can include ordering the respondent to cease impersonating the petitioner, or to cease using the petitioner's personal information and/or photograph. Listing specific examples, such as prohibiting posting on a website, can help in enforcement, but the language should also include general terms.

Remedying financial identity theft takes time and money. Compensation should be sought in a Civil Protection Order, similar to other damages. The abuser could also be ordered to turn over items or compensation for items acquired via identity theft, which have left the petitioner with a credit account debt.

Another potential remedy is to place limits on how the respondent may gain access to the petitioner's personal information. In California, the protection order form contains language that orders the respondent not to "[t]ake any action, directly or through others, to get the addresses or locations of any protected persons or of their family members, caretakers, or guardians."[11] Expanding this protection to other personal information, such as phone numbers, social security numbers, or email addresses will aid in the prevention of identity theft as well as promote petitioner's safety. In one case, the abuser posted the victim's phone number in an online forum, impersonating her and seeking anonymous sexual encounters in the middle of the night. This caused her to receive several harassing phone calls. She later changed her phone number, and the abuser called her workplace trying to find out her new number. In the final order, the abuser was ordered not to seek out her new number. This prevents the abuser from gaining a tool of harassment – her number – and also prevents calls to her workplace seeking her number. Introducing evidence of past misuse of personal information, past self-defense measures (such as changing phone numbers) and past attempts by the abuser to bypass this self defense all strengthen the case for this sort of remedy.

Resources

Federal Trade Commission [http://www.ftc.gov/bcp/edu/microsites/idtheft/]

Annual (free) Credit Reports [http://annualcreditreport.com/]

Identity Theft Resource Center [http://www.idtheftcenter.org/]

Privacy Rights Clearing House: Identity Theft Fact Sheets [http://www.privacyrights.org/identity.htm]

---

[1] Margaret Reardon & Anne Broache, *FCC Imposes New Rules Designed to Prevent Pretexting*, CNet, April 2, 2007, http://news.cnet.com/2100-1037_3-6172705.html.

[2] Telephone Records and Privacy Protection Act of 2006, Pub. L. No. 109-476, 120 Stat. 3568.
[3] *See* Electronic Privacy Information Center, *The Amy Boyer Case: Remsburg v. Docusearch*, http://epic.org/privacy/boyer/.
[4] *See* Federal Trade Commission, *Your Access to Free Credit Reports,* http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm, ("[Y]ou're entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.").
[5] Federal Trade Commission, *Free Annual Credit Reports*, http://www.ftc.gov/freereports. Be careful of other websites offering "free credit reports" – some have been sued by the Federal Trade Commission for deceiving consumers. *See, e.g.*, Federal Trade Commission, *Marketer of "Free Credit Reports" Settles FTC Charges*, Aug. 16, 2005, http://www.ftc.gov/opa/2005/08/consumerinfo.shtm
[6] 15 U.S.C. § 1681j.
[7] Federal Trade Commission, *Defend: Recover From Identity Theft*, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html.
[8] Consumers Union, *Consumers Union's Guide to Security Freeze Protection,* http://www.consumersunion.org/campaigns//learn_more/003484indiv.html.
[9] The Smoking Gun, *Felony Charge for Craigslist Prank*, March 5, 2009, http://www.thesmokinggun.com/archive/years/2009/0305094eau1.html.
[10] Wis. Stat. § 943.201(2)(c).
[11] California Courts, *Restraining Order After Hearing (Order of Protection)*, DV-130, http://www.courtinfo.ca.gov/forms/documents/dv130.pdf.