Hal Berghel

WAYS WE INVITE IDENTITY THEFT

Reality: Jay receives a call on his cell phone from BANCOPAL: "You've had 5 ATM withdrawals on your debit card in the past 24 hours from three ATM machines in Portland for $2,140. We're just checking to verify that these withdrawals are authorized." Jay: "I've been in Miami for the past week and my debit card is in my hand. These charges were unauthorized and not made by me." BANCOPAL: "Ok, we'll cancel this card. You should receive a new debit card and PIN in separate mailings within 6-10 business days. Call the 800-number on the sticker to activate your new card."

Jay is sure relieved. "Who could be doing this?" he wonders. How did they get a copy of his debit card? Why, I'm sure glad that my local bank, BANCOPAL, is looking after me."

Imagine Jay's surprise when he sees the $2,140 debit on the next account statement. He calls BANCOPAL to explain their error, only to get his second lesson in Identity Theft 101. The bank reports that the fact that the thief used Jay's PIN, which was only known to Jay and should have been under his care, custody and control. The fact that someone else knew it is presumptive evidence that the compromise in security (and liability) was at Jay's end. BANCOPAL also volunteers that they've checked their computer logs and that there was no security compromise of any of BANCOPAL's computer systems and the logs of the remote ATM betrayed no suspicious activity. Note: No matter what the eventual outcome, Jay will eat the loss for the time sink and any attorney's fees - not to mention the $2, 140 if his attempt to dump this on BANCOPAL is unsuccessful.

In our second example, Sally gets a call from Stores R Us indicating that her account is in arrears. That's funny, Sally thinks to herself. She recalls that she cancelled her Stores R Us credit card over a year ago. Discussion with Stores R Us indicates that someone re-opened Sally's account and subsequently charged against it. The individual provided Sally's contact information (physical address, phone, and email), her employer's name, address and phone, and even Sally's original account number. If there's something wrong, it must be at Sally's end. "Who did you give this information to?" Stores R Us inquires. "You should be more careful with this information. If you wish to dispute this bill, you'll need to download, complete, and return several forms from the Stores R Us corporate website and provide a copy of a completed and signed police report." Note: Like Jay, Sally is likely to take the pipe on lost time and attorney's fees. It's her responsibility to prove that she isn't the culprit.

The Genesis of the Problem

The genesis of this problem is twofold. First, there are criminals out there who prey on unsuspecting victims. There's a news flash! Second, and more importantly, there is precious little incentive for businesses and government to help us protect ourselves against digital crime. Not only don't they help much, they actually work against our interests.

A little background is in order. Accompany me to the dark side of the world of plastic. Credit and debit cards are considered "same as cash" by criminals. The modus operandi is called "carding," slang for converting plastic to cash. The primary target is called a "full" which is the card number, billing address, and any security code on the back of the card. The holy grail of this form of thiefdom is called the COB - which stands for "change of billing" information. A COB is a full augmented with Password or PIN.

As far as the criminal is concerned, there is no difference between a credit and debit card - both can yield carding. But there is a huge difference to the cardholder. Unlike credit cards, debit cards provide a direct access into the cardholder's bank account. Fraudulent charges are withdrawn directly from savings, not a 3rd party credit card company armed with an arsenal of private investigators, attorneys, and the clout to shut down credit lines. Individuals and their bank accounts are at their most vulnerable because when they become victims, they're on their own.

How did Jay get into this fix? He undertook unnecessary risk: he used a debit card. I have been telling audiences for years that debit cards belong in a safe, not a wallet. What we do know is that the criminals are always finding new ways to compromise credit/debit instruments, from placing "invisible" readers and cameras on ATM machines, to capturing point-of-sale transmissions, to "card skimming" in restaurants. Smart money understands this vulnerability.

Jay put himself at additional risk by using debit cards when credit cards would suffice, thereby denying himself the opportunity to refuse the transaction. Financial institutions could ameliorate this problem by fully disclosing the increased risk of using debit cards vs. credit cards on the top of the application form. They don't do this because it is profitable for them to encourage customers to take on the additional risk. Remember, the protections that credit cards afford the card holder are not available to debit card holders.

Sally's case is a bit different. In this case, there's not much more that Sally could have done to protect herself. She is a victim of Stores R Us' hunger for business. They have decided that their margins are high enough that they can accommodate losses that might result from easy credit, so they've relaxed their requirements - much to Sally's chagrin. But notice the illogic concerning the burden of proof of the fraud: Stores R Us told Sally that the responsibility falls on Sally to prove that she's not responsible for the charges. That's some twisted logic for you. Because Stores R Us has virtually no standards regarding the issuance of credit, Sally takes a big hit on her time and possibly budget. This is an example of having the shoe on the wrong legal foot. In any reasonable legal system, it should be the responsibility of the merchant to prove that Sally had the card reissued, not the other way around. If you have any doubts about this, drill down a few layers on PIPL.COM and see how easy it is to personal information on your neighbors! Satisfy yourself that reopening credit accounts has few safeguards for the victim.

What Can We Do to Protect Ourselves?

Someone, somehow, got access to Jay's debit card information. Jay's case is also the easiest to solve: kibosh the debit card. Something in his debit-card-world is awry, and until he gets it in order the best thing he can do for himself is stick to cash, check and credit cards. And even when he does get his world in order, he should give serious consideration whether and to what extent he really wants to undertake the additional risk of using debit cards, recognizing full well that he places himself at the mercy of his bank should irregularities arise.

Sally's case is somewhat more complicated. This is a case of perpetrator account creation, but with a victim account reactivation twist. Sally did everything right, and still got zapped. Picture a balance with Sally picketing Congress on one scale, and the business lobbyists offering campaign contributions on the other. I'm not seeing Sally winning this one. By the way, there's something of an analog with pre-approved credit. The law holds that the recipient (including your 7-year old and family pet) cannot be held to accept by silence or inaction *unless* there is a pattern of acceptance. This means that if your 7 year old accepted pre-approved credit once before, then there may be implied acceptance for subsequent offers. Take note if your 7 year old is routinely picking up the tab for school snacks!

As a general practice, Sally (and anyone else) should give careful consideration to using some of the Federal Trade Commission services for free annual credit reports, fraud alerts and credit freezes, depending on circumstances. The applicable laws seek to balance business interests with individual rights, so they don't always make prima facie sense, but they're better than nothing.

Fraud alerts place flags in the credit records that are held by the big-3 credit services companies, Experian, Equifax, and TransUnion. The idea of a fraud alert is to require potential creditors to take reasonable steps to establish proof of identity. To my way of thinking, that should be the default, but then I don't receive campaign contributions from business lobbies. The way it works in practice is that an initial fraud alert only lasts for 90 days. This was a concession that Congress made to business interests who wanted to minimize their inconvenience when issuing credit. The more useful 7-year extended fraud alert requires that you jump through a multitude of hoops, not the least of which is providing "proof" that you have actually be the victim of identity theft. An extended fraud alert also triggers a "block" on pre-approved credit offers (which I feel should be a right of citizenship, but no one asked). Perhaps of greater use is the "credit freeze" that restricts access to credit reports. This feature helps because the identity thief can't get credit under your name because the potential credit issuer can't gain access to your credit report. All states but Alabama, Michigan and Missouri require credit reporting companies to allow individuals to protect their credit with a credit freeze. In my state, Nevada, a credit freeze is free if the request accompanies a police report; else $15. A charge of $18 is required to lift the freeze, and $20 to lift it temporarily for one creditor. Charges and expiration dates vary from state to state.

Fraud alerts and freezes are similar to Opt-Out Lists and DoNotCall registries - they're usually good ideas even though they don't work very well - have you seen any decrease in spam lately?. There's really not much of a downside to the consumer beyond slowing the process of approving credit. The reader should understand that any of these means will raise the barrier when it comes to obtaining credit.

Good luck.

Hal Berghel is Associate Dean of the Howard R. Hughes College of Engineering at UNLV and Director of the new UNLV School of Informatics. He is also Director of the Identity Theft and Financial Fraud Research and Operations Center. His consultancy, Berghel.Net, provides security and management services to government and industry.