

TABLE 2: TECHNIQUES TO REDUCE IDENTITY THEFT

Increase the Effort	Increase the Risks	Reduce the Rewards	Reduce Provocations	Remove Excuses
<p><i>Target harden</i></p> <ul style="list-style-type: none"> ▪ Tamper proof credit cards ▪ Firewalls ▪ Tamper proof ID documents ▪ Shred utility bills etc. <p><i>Control access to facilities</i></p> <ul style="list-style-type: none"> ▪ Lock mail boxes ▪ Card/password access to ID databases ▪ ID for mail forwarding ▪ Disallow remote access to databases ▪ Limit number of persons with access to ID databases <p><i>Deflect offenders</i></p> <ul style="list-style-type: none"> ▪ Require several forms of ID to obtain new ID or replacement. <p><i>Control tools/ weapons</i></p> <ul style="list-style-type: none"> ▪ Control sale of ID making equipment (card readers, strippers, printers) ▪ Use tracking ID tags to track location of use and who uses machine 	<p><i>Extend guardianship</i></p> <ul style="list-style-type: none"> ▪ Close scrutiny, background checks of employees with access to ID databases <p><i>Assist natural surveillance</i></p> <ul style="list-style-type: none"> ▪ ATMs in well lit areas ▪ Disallow employees to take work home ▪ Support whistleblowers <p><i>Reduce anonymity</i></p> <ul style="list-style-type: none"> ▪ Photo, thumb print on ID documents, credit cards ▪ Require additional ID for on-line purchases ▪ Train clerks, police, officials in document authentication procedures <p><i>Utilize place managers</i></p> <ul style="list-style-type: none"> ▪ Reward vigilance for supervisors of employee/customer records <p><i>Strengthen formal surveillance</i></p> <ul style="list-style-type: none"> ▪ Retain backup files of computer usage ▪ Track keystrokes of computer users ▪ Monitor all utilization of ID databases ▪ Cameras on ATMs, at check-out counters, shipping and mailing services, ID granting agencies ▪ Background checks of employees 	<p><i>Conceal targets</i></p> <ul style="list-style-type: none"> ▪ No social security numbers on health, school cards ▪ No credit card numbers on receipts ▪ Place ATMs so keystrokes cannot be observed or recorded ▪ Shred utility bills <p><i>Remove targets</i></p> <ul style="list-style-type: none"> ▪ Pre-paid cards for pay phones ▪ Smart cards that contain limited personal ID information ▪ Do not leave wallets in cars <p><i>Identify property</i></p> <ul style="list-style-type: none"> ▪ Guaranteed ID authentication services (e.g. Microsoft Passport) ▪ Vehicle ID licensing and parts marking <p><i>Disrupt markets</i></p> <ul style="list-style-type: none"> ▪ Monitor pawn shops ▪ Monitor retail returns departments ▪ Monitor deliveries to vacant houses ▪ Monitor classified ads. <p><i>Deny benefits</i></p> <ul style="list-style-type: none"> ▪ Swift notification of stolen credit card 	<p><i>Avoid disputes</i></p> <ul style="list-style-type: none"> ▪ Maintain positive management-employee relations <p><i>Reduce arousal and temptation</i></p> <ul style="list-style-type: none"> ▪ Avoid public disclosure of security holes and patches in software ▪ Do not boast of security features in software 	<p><i>Set rules</i></p> <ul style="list-style-type: none"> ▪ Responsible computer use policy <p><i>Post instructions in college dorms, workplace</i></p> <ul style="list-style-type: none"> ▪ "Respect Privacy" ▪ "Protect our customers' privacy" <p><i>Alert conscience</i></p> <ul style="list-style-type: none"> ▪ "Hacking hurts people" <p><i>Assist compliance</i></p> <ul style="list-style-type: none"> ▪ Provide shredders for employees

Adapted from Clarke and Eck (2004) and Clarke (2004).