AT&T Wireless Services

Testimony Before

The United States Sentencing Commission

Identify Theft Act
&
Wireless Telephone Protection Act

Roseanna DeMaria
Senior Vice President
Business Security

AT&T Wireless Services
32 Avenue of the Americas
Room 1731
New York, NY 10013
Office: 212 830-6364
Fax: 212 334-12221

Technological Convergence Warrants Uniform Sentencing Irrespective of the Technology Used For Theft or Access

Thank you for the opportunity to share with you our views of the proposed sentencing options for the Identity Theft Act and the Wireless Telephone Protection Act. These 1998 acts provided a proactive approach to the evolving criminal of the millennium who relentlessly capitalizes on technology for illicit purposes to victimize the American consumer and industry. We support the approach embraced by Option 3 and applaud its clear attempt to address the rapidly changing criminal frontier of the millennium through a wide view of "access device" and a revisitation of loss amounts for sentencing. Option 3 comes closest to our view that sentencing for Identity Theft and access device creation-and-use must be based on broader principles than simply the amount of dollar loss. Indeed, dollar loss is an inappropriate measure altogether because it fails to consider the impact on the integrity of the system, consumer confidence in that system, and the privacy and rights of individuals. Quite simply, the future demands a better measurement tool than monetary loss. While we support Option 3, we urge the United States Sentencing Commission to revisit Identity Theft from a holistic perspective. It is a significant threat to marketplace competition, the American consumer and our fundamental constitutional values of property and privacy.

We respectfully submit that the current marketplace is exploding with competition and technological convergence to birth multiple generations of products and services for the American consumer. This explosion has been encouraged by the FCC and aggressively pursued by the telecommunications industry. This is the context for the Internet explosion along with all Internet-related services. E-commerce brings to us a new, ubiquitous approach to all transactions, both consumer and business. On-line trading and on-line banking will change the landscape for financial institutions. The convergence of voice and data through wireless and broadband will similarly change the way we conduct our lives. These areas are but a portion of the landscape. For this landscape to grow and advance the consumer must have confidence in it. Identity Theft exponentially threatens that confidence and undermines our basis constitutional values.

As a result of this technological convergence, there needs to be a uniform approach to penalizing Identity Theft. It is irrelevant whether the access proliferating the Identity Theft is from a mobile terminal, a fixed computer, or an ATM - the problem is the same - the security of the experience is threatened because of the compromise of constitutional property and privacy values. Consumer confidence will be irreparably harmed. The criminal capitalizes on these technological opportunities to maintain anonymity through Identity Theft. Just as technological development advances at the speed of Internet time, the criminal of the millennium advances equally fast. Despite Congress' best efforts to keep pace with this criminal, it will never be able to legislate at Internet speed. Accordingly, the criminal has an advantage.

To date, Congress has aggressively focused on proscribing technology-specific crimes. Uniform to those crimes is one, robust approach, namely: the rapid evolution and proliferation of Identity Theft across technologies in pursuit of anonymity to commit other crimes. The penalty for this criminal methodology must be consistent in its message to all crimes. The impact of this crime on consumer confidence, and ultimately on value in the marketplace, cannot be overstated. This can be done in the sentencing approach as opposed to sentencing focused on each, individual,

technology-specific statute. Increased sentencing penalties, with appropriate gradations based on constitutional values, for any criminal act where Identity Theft is part of the modus operandi would send a clear message of deterrence and zero tolerance.

The future is here for this criminal approach. Presently, we are seeing the growth of Identity Theft. The Federal Trade Commission recently initiated a toll free hotline for Identity Theft calls. This hotline is already logging 400 calls a week. The Federal Trade Commission is forecasting an annual call volume of 200,000 calls a year. Similarly, the General Accounting Office reports an increase in inquiries to the Trans Union credit bureau's Fraud Victim Assistance Department from 32,235 in 1992 to 522,922 in 1997. The Social Security Administration Office of the Inspector General conducted 1,153 social security number misuse investigations in 1997 as compared to the 305 investigations conducted in 1996. 81% of these cases involved Identity Theft. Similarly, recent evidence suggests that organized Chinese fraud rings are currently turning to hacking techniques and Internet theft to obtain identity information through compromising credit and identity databases as opposed to more traditional methods. The trend on this changing criminal frontier is clear. Identity Theft is the franchise player on the criminal team of the future.

The emergence of cloning in the wireless industry taught us that criminals were interested in "anytime anywhere" communications when anonymity was involved. Prior to cloning the criminal used Identity Theft through subscription fraud to obtain a anonymous wireless usage. Unlike traditional theft of services, the majority of these criminal "customers" were not interested in stealing service. They were interested in anonymous usage to ply their illicit trades and evade law enforcement detection. The industry loss numbers profoundly demonstrate the scope of this criminal demand. In 1995 that demand reached its height at 3.8% of industry revenue. These numbers are relevant because they reflect the massive size of the criminal demand. While cloning has steadily decreased and is de minimus in the face the industry's technological solutions, the criminal demand remains. That demand is reflected in the current proliferation of Identity Theft. This conclusion is profoundly demonstrated by the above statistics.

Loss amounts have factored prominently in sentencing to measure the crime's impact and to determine the corresponding penalty. These amounts are necessary in traditional theft crimes. The above-described changing criminal frontier requires a different view. The amount of money lost in a clone phone call cannot even approximate the impact of that crime. When that clone phone call orders a murder, directs a kidnapping or manages a criminal enterprise with anonymity, the loss amount becomes irrelevant. While 3.8% of industry revenue is a significant number, it also does not reflect the complete impact of the 1995 cloning hemorrhage. Every time a customer becomes a cloning victim, their property and privacy rights are violated, and their confidence in technology is shaken. The theft of an ESN/MIN combination is difficult to conceptualize from a conventional constitutional perspective because the ESN/MIN combination is not a tangible piece of property. The invasion of privacy, however, becomes even greater because of this fact.

Accordingly, we submit that the quantification of the damage in an Identity Theft crime is adversely impacted from a loss amount analysis because the latter is measuring a clearly quantifiable commodity - dollars. Far more than dollars is lost in Identity Theft. The use of an average loss amount or a presumption cannot reflect the gravity of this crime's impact in the situation where a criminal has harvested hundreds of ESN/MIN combinations but had not used the cloned phones containing them at the time of arrest. This is not a victimless crime because the loss

amount is zero. The intrusion of property and privacy rights is no less significant because the loss amount is zero. Our view of Identity Theft is based on this perspective

Moreover, the dependency on monetary loss amounts to determine offense levels does not conform with the notion that there need not be a direct "victim" (i.e., a person/entity which suffers a quantifiable monetary loss) in order for certain behavior to constitute a violation of either the Identity Theft Act or the Wireless Telephone Protection Act. For example, the mere possession of the specialized equipment necessary to clone a wireless telephone can constitute a violation of § 1029, regardless of the fact that there is arguably no tangible "victim" in a case where a phone is not actually cloned. See 18 U.S.C. § 1029(a)(9). In revising 18 U.S.C. § 1029 in 1998, Congress recognized that cloning had become a pervasive problem that justified a revision of the statute to strengthen the power of federal authorities to prosecute such crimes. These revisions included the removal of the "intent to defraud" requirement in connection with the use, production, custody, or control of a cloning device because, in practice, such intent requirement impeded the efforts of law enforcement to prevent, among other things, the cloning of telecommunications devices. H.R. Rep. No. 418, 105th Cong., 2nd Sess. 1998, 1998 U.S.C.C.A.N. 36-1.

Options 1 and 2 of amendment 5, intended to address the Identity Theft Act, recognize this broader notion of harm in the context of Identify Theft crimes by providing automatic enhancements and a minimum base level regardless of the actual monetary loss if the crime involves the use or possession of certain identification information. While this is certainly a step in the right direction, both options still fail to consider full impact of Identity Theft crimes on the individual and the economy. Option 2 is clearly preferable, as it recognizes the impact of such a crime on the individual victim beyond monetary loss (i.e., loss of reputation and credit standing). Even this option does not consider the effect of an Identity Theft crime beyond those on a person's reputation or credit history. As I indicated above, when a person's identifying information is appropriated, his or her confidence in the ability of the telecommunications industry and the Government to protect his or her property and privacy interests is also severely damaged, regardless of the impact on credit history or other such records. Cf. 114 Cong. Rec. S3019-03, S3020 ("Wireless fraud is not a victimless crime. It strikes at the heart of technology that is improving the safety, security and business productivity of the entire Nation."). This broader harm is not accounted for in either option.

Options 1 and 2 of amendment 6, proposed to address the Wireless Telephone Protection Act attempt to address the concern, embodied in the law, that I raised earlier: the mere possession of equipment that has been configured to clone, is equally as repugnant to the statute as the actual use of such devices. Option 2 is clearly preferable to Option 1, because it provides enhancements for the possession of equipment to produce any "access device" as defined in the statute and not just "cloning equipment." This not only takes into account the possessory penalty of § 1029, but also the fact that "cloning" is not the only fraud crime faced by the wireless industry. Option 2 also accounts for the problem of persons who appropriate identification information such as an ESN/MIN in order to, among other things, remain anonymous in committing other crimes. By incorporating such use, the Commission has implicitly recognized the concern expressed by Congress when revising the Wireless Telephone Communications Act in 1998 -- that cellular telephone fraud is not perpetrated just to sell cloned telephones, but rather to advance other criminal actions:

> As significant as is the loss of revenue to the wireless telephone industry, cellular telephone fraud posses another, more sinister, crime problem. A significant amount of the cellular telephone fraud which occurs in this country is connected with other types of crime. In most cases, criminals used cloned phones in an effort to evade detection for the other crimes they are committing. This phenomena is most prevalent in drug crimes, where dealers need to be in constant contact with their sources of supply and confederates on the street.

H.R. Rep. No. 418, 105th Cong., 2nd Sess. 1998, 1998 U.S.C.C.A.N. 36-1.

This last point - the misappropriation of ESN/MIN information that qualifies both as identification information under the Identity Theft Act and an access device under the Wireless Telephone Communications Act - highlights another fundamental problem with both of the options under the proposed amendments 5 and 6. None of the proposals published on February 10, 2000 take into account the interrelationship between the two acts. In defining what constitutes a "means of identification" for the purposes of § 1028, Congress specifically included "telecommunication identifying information or access device (as defined in section 1029(e))." 18 U.S.C. 1028(d)(3)(D) (emphasis added). Only Option 3 reflects this interrelationship, and offers a combined Guideline. While Option 3 still conceptualizes the harm from these crimes too narrowly by focusing on monetary loss, it appropriately provides for a higher minimum penalty for those who violate the act without any direct monetary impact on any individual.

As a means of correcting this dependence on monetary loss in the determination of appropriate penalties, in addition to the enhancements proposed in Option 3, we respectfully suggest that the Commission consider raising the Base Offense Level contained in § 2F1.1 from 6 to 8 (with a resulting minimum base level of 14 under § 2F1.1(b)(5) of Option 3) to reflect the seriousness of these violations both to the victims of such crimes as well as the telecommunications industry and the economy as a whole. Such a revision would also bring the potential penalties in § 2F1.1 more in line with those contemplated in other sections of the Guidelines that address consumer protection statutes.

For example, § 2N1.2 of the Guidelines - which addresses the giving of false information about or threatening to tamper with consumer products - provides for a base offense level of 16. Actual tampering that results in the risk of bodily injury has a base level of 25. The base level for violations under the Identity Theft Act and Wireless Telephone Protection Act, in contrast, is 6 (when taking into account the departures set forth in Option 3), even though both Acts are designed in part to protect broader consumer interests. Similarly, § 2Q1.2 - which concerns mishandling even minimal amounts of hazardous or toxic substances, or failure to keep accurate records - has a base offense level of 8, the level which we propose be applied to § 2F1.1. Substantial increases above the proposed base level should be considered where the threat of or actual harm to privacy interests is great, even though monetary loss may not be quantifiable, e.g. wholesale harvesting of ESN/MIN combinations.

The sentencing approach in Option 3 set forth above deserves support because it is forward-looking. Fundamental to this approach is a recognition that Identity Theft is a toxic gas that will expand to fit the container of existing technological opportunity. Accordingly, the sentencing view that contemplates all access devices is appropriate. Similarly, a view of loss that

attempts to measure risk by expanding the minimum loss rule and increasing the loss amount is meaningful, albeit limited. These changes are only a first step. The reality of the changing criminal frontier of the millennium is that we must recognize that Identity Theft is in the critical path of success for technology and value to the consumer. Identity theft has always threatened our constitutional values of property and privacy. In the current state of technological convergence, however, this threat is exacerbated to a crisis-level. It must be contained and deterred, or it will undermine the explosion of value to the consumer provided by marketplace competition, the Internet and its attendant-related services. This crime will erode our constitutional framework in a manner that we have never experienced before.

We urge the United States Sentencing Commission to create a uniform approach to sentencing for crimes involving Identity Theft that reflects the degree of criminal intent and the resulting erosion of property and privacy values regardless of the crime charged. It is an aggravating factor that warrants special treatment. The promise of convergence and new technology will never be realized if consumers don't accept it due to fear that their identity and the most personal aspects of their lives are at risk. Sentencing that recognizes this harm as well as the other costs is appropriate and necessary to prevent and deter future criminal behavior and to reflect the gravity of the offense for which the criminal has been convicted. The changing criminal frontier demands it, our constitutional values mandate it, and the American consumer deserves nothing less.