

Melissa Beyer
Steve Eberlein
Professor Hoar
Cybercrime – Identity Theft

IT'S ABOUT TIME: PUNISHING IDENTITY THIEVES IN CYBERSPACE

As soon as the final futon bed is unloaded and the last minivan departs campus, the four-year haze of college begins for tens of thousands of teenagers across the country. As nervous freshman creep out of their dorm rooms struggling to make the most of their newly acquired freedom, one member of the pack immediately emerges to take to a leadership position. He's the guy named Chad at the end of the hall. He's the one with the least acne and the most facial hair. He's probably wearing tattered jeans, a faded Budweiser t-shirt without sleeves, and he has his hat on backwards. But most importantly, he's got the expired driver's license of Rick, his 23-year-old brother. He can get the beer, so everyone wants to be his friend. Life is good for Chad.

Oh, for the good old days of identity theft.

Although the scene described above is admittedly an over-simplified look at pre-internet identity theft, it does speak to the sort of crimes early identity theft legislation was aimed at preventing. To that end, 18 U.S.C. §1028 was a rather efficient statute, and provided federal prosecutors with a functional tool to reasonably punish criminals charged with fraud and related activity in connection with identification documents, authentication features, and information. However, as the internet gained popularity, identity theft became easier to commit, the rewards of identity theft increased dramatically, and the likelihood of apprehension or serious punishment declined. By the turn of the century, identity theft was being referred to as the crime of the new millennium in many circles.¹

The results of a 2003 survey conducted by the Federal Trade Commission (FTC) indicated that nearly 10 million Americans had become victims of identity theft in the preceding year.² From 2001 to 2003 identity theft complaints to the FTC nearly tripled, from 86,212 to 214,905.³ In July of 2004 President Bush placed a \$50 billion price tag on identity theft in the United State alone.⁴

¹ *Identity Thieves*, REG. GUARD (Eugene, Or.), Apr 30, 2000, at 1A.

² Testimony of Timothy Coleman..

http://www.globalsecurity.org/security/library/congress/2004_h/coleman032304.htm

³ *Id.*

⁴ <http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html>

The increase of occurrences, victims, and economic losses to individuals and businesses was staggering. However, prosecutors were still trying to combat this new breed of identity theft with an embarrassingly outdated 18 U.S.C §1028(a)(7). Even in cases where the criminals could be apprehended and tried, often times they would get off with probation or less. This was due in large part to the Federal Sentencing Guidelines inability to function in an internet-heavy economy.

Take for instance a “phishing” scheme. By sending out fraudulent emails purporting to be a reputable financial institution, one criminal could steal millions of dollars from hundreds of victims. However, if a prosecutor could not identify and locate these victims, the criminal could walk with probation. This had citizens, prosecutors and legislatures complaining that “the time didn’t fit the crime.”

On July 15, 2004 President Bush signed H.R. 1731, better known as the “Identity Theft Penalty Enhancement Act.”⁵ The result of this was a revision of 18 U.S.C. §1028 and the creation of 18 U.S.C. §1028(A), or the Aggravated Identity Theft Statute. The concept behind this bill was simple: close the loopholes the internet had exposed in the Identity Theft Statute. The focus of the remainder of this paper will be the Aggravated Identity Theft Statute.

Conscious of the pitfalls of relying on the Federal Sentencing Guidelines, Congress drafted a statute that would make Aggravated Identity Theft a “derivative offense.” In other words, if a criminal used stolen identities or identification materials during or in relation to a specified felony, they could also be charged with Aggravated Identity Theft under the new statute. This was modeled after 18 U.S.C. §924(c), a statute criminalizing the carrying of a firearm in a violent or drug trafficking crime.⁶ In the same vein, 18 U.S.C. §1028 enumerates a variety of felonies that will trigger the Aggravated Identity Theft charge, they include crimes relating to: theft of public money; false personation of citizenship; false statements with the acquisition of a firearm; mail, bank, and wire fraud; and violations of the Social Security Act.

However, criminalization of this activity was only half of the answer. The Federal Sentencing Guidelines are generally “charge-neutral:” in other words sentencing only relied on the criminal’s “relevant conduct” in the commission of the crime. One result of this system is that an increased number of convictions the defendant faced didn’t necessarily equate to a stiffer sentence. To remedy this problem, mandatory sentences were included in the language of the new Aggravated Identity Theft statute. Specifically, a mandatory two-year additional sentence was included for every conviction under 18 U.S.C. §1028(A). In cases where the underlying criminal conviction could be traced to a terrorism offense, the mandatory sentence jumped to five years incarceration.

Determined to give the new statute “teeth,” the drafters included three other provisions dealing with the sentencing of criminals under the statute: 1) the court could not place anyone convicted under the statute on probation; 2) the court could not consider the

⁵ *Id.*

⁶ Testimony of Timothy Coleman

additional sentence when sentencing the criminals for the underlying felonies; and 3) sentences under the statute could not run concurrently with other sentences. (With one notable exception: if the defendant was convicted of multiple counts of aggravated identity theft, the mandatory sentences could be run concurrently at the judge's discretion. This was added to guarantee that the statute would not become too rigid and un-workable.)

Three years after the adoption of 18 U.S.C. §1028(A) convictions of identity thieves are up, and in most cases the sentences better reflect the damage caused by the crime. Not surprisingly, however, there have also been speed bumps along the way.

One of the more noteworthy debates in the Federal Circuit Courts right now seeks to answer the following question: "Can a defendant plead guilty to a single count of aggravated identity theft with out entering a plea to the underlying predicate felony enumerated in 18 U.S.C. §1028(A)?"

The benefits of this are rather straightforward. Prosecutors could strike deals more readily with defendants, thereby saving time, money and resources for other endeavors. It may also avoid appellate reversals under 18 U.S.C. §1028(A) when there is no conviction for the predicate felony.

As the debate stands now, there appears to be a return to the Aggravated Identity Theft Statute's relation to 18 U.S.C §924(c). Given that the firearms statute lent its form to 18 U.S.C. §1028(A), the judicial treatment of the firearms statute carries much weight in this discussion. In a case decided in the 4th Circuit Court, the court held that a defendant can plead guilty to a derivative offense without entering a plea in the predicate felony.⁷ It appears as though this will be the path of the Aggravated Identity Theft Statute.

⁷ *United States v. Crump*, 120 F.3d 462, 466 (4th Cir. 1997).