CORPORATIONS: STUCK WITH THE WHITE COLLAR CRIME CHECK

PROFESSOR ELLEN S. PODGOR*

Introduction by Professor Lucian Dervan

Professor Dervan. I have the great pleasure and honor of introducing our keynote speaker for today's event, Professor Ellen Podgor from Stetson University College of Law.

Professor Podgor holds the Gary R. Trombley Family White Collar Crime Research Professor of Law position as one of the world's leading experts in this field. She is both a former deputy prosecutor and a criminal defense attorney, and she now teaches in the area of criminal law and procedure and white collar crime. She is the co-author of numerous books including: *White Collar Crime in a Nutshell*, *Understanding International Criminal Law*, *Mastering Criminal Law*, *White Collar Crime Hornbook*, *Mastering Criminal Procedure I* and *II*. She has also authored more than seventy law review articles and essays in addition to being the founder and editor of the well-known White Collar Crime Prof Blog.

In addition to her scholarship and teaching, Professor Podgor is actively involved in a number of organizations and projects. For example, she is Chair of the Advisory Committee of the NACDL White Collar Criminal Defense College at Stetson, served for six years as a member of the Board of Directors of the NACDL, and as a member of the American Law Institute. I could go on and on, but I will conclude by mentioning just one more of Professor Podgor's many achievements and honors.

In 2010, I was honored with introducing Professor Podgor at the ABA Criminal Justice Section Fall Awards Luncheon where she received the Raeder-Taslitz Award, an award given each year to a law professor who has, among other things, made a significant contribution to promoting public understanding of criminal justice and best practices on the part of lawyers and judges. Professor Podgor certainly exemplifies all of these traits.

---

* After receiving her Bachelor of Science from Syracuse University and her Master in Business Administration from the University of Chicago, Ellen S. Podgor earned her Juris Doctor degree from Indiana University at Indianapolis before earning her Master of Laws at Temple University. In addition to serving as a deputy prosecutor and criminal defense attorney, Podgor has been interviewed on National Public Radio and quoted in national newspapers, including the Wall Street Journal, Business Week, the New York Times, and National Law Journal. She now teaches in the areas of white collar crime, criminal law, and criminal procedure at Stetson University's College of Law.

And so, please join me in welcoming an incredible scholar, and my dear friend and mentor, Professor Ellen Podgor.

Professor Ellen Podgor. Good morning and thank you very much Professor Dervan. It is a real pleasure to be here at Belmont College of Law. I would particularly like to thank all the students of the Law Review. I have been most impressed with their professionalism, which has made this a wonderful experience for me.

My credit card was hacked. It's not the first time my American Express credit card was hacked. It happened to me two times in the last ten years. No, I didn't buy over One Thousand ($1,000) Dollars' worth of shoes, nor the items from Frederick's of Hollywood.

My MasterCard was also hacked one time. They could have at least invited me on the over Seven ($700) Hundred Dollar Uber ride they took in the wine country of California, while I was home in Florida.

Each time it was a bit of a nuisance to me – changing my automatic subscriptions, waiting for a new card to arrive.

But it cost me nothing. I didn't pay a dime. It was not my concern. It was not my problem.

ACI Worldwide, "an electric payment system company" "estimates that 46% of Americans have had their [credit] card information compromised at some point in the past five years."[1] And with the use of the new cards using EVM chips, that number has gone down for in-person credit card fraud. But the number has gone up for online credit card breaches[2] and more importantly, data breaches – these have significantly increased.[3]

Sometimes the loss can be to the person – perhaps also to their credit rating as they straighten out the mess caused by the theft of the card. And when they take the entire identity of a person, or perhaps their passport number and information, the damage can be even worse.

But when it happened to me, it was not my problem.

---

[1] *See* Rebecca Lake, *23 Frightening Credit Card Fraud Statistics,* at 2, Feb. 1, 2017, *available at* https://www.creditdonkey.com/credit-card-fraud-statistics.html. (last visited April 22, 2019).
[2] *Id.* at 3.("While [EMV] helps with reducing in-store fraud, it doesn't help online fraud. If fact, this just make fraudsters target new accounts (as opposed to existing accounts). By the end of 2015, there was a 113% increase in new account fraud, which accounted for 20% of all fraud losses.")
[3] *Id.* at 4; *see also* Jason Steele, *Credit Card Fraud and ID Theft Statistics*, Oct. 24, 2017, *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php. (last visited April 22, 2019).

In one case – the Fredericks of Hollywood – the card company realized it didn't fit my profile and contacted me immediately. And in the case of the shoes, the UPS notice telling me my package was on its way to some residence other than mine – was an immediate clue to check on what this package actually was, since it was clearly not something I ordered.

But is this fraud? Is it theft? Is it white collar crime? And who's paying the check? Yes, who is taking the loss? And is it unique that our corporations and banks are being stuck with paying the tab when criminal activity occurs? These are the questions that I would like to look at today.
Yes, much of our enforcement policy has moved from the assigned enforcers over to the large corporations, financial institutions, and yes, even the small businesses that struggle to keep their doors open. What I am going to talk about is why it is important to put more government funds into enforcement.

So, the three things I am going to talk about today are whether -
First - Is this white collar crime?
Second - Who is paying the tab for this criminality?
And Third - Do we need to change the current enforcement methodology?

Looking at the first question - Is this white collar crime?

White Collar Crime is a term coined by Edwin Sutherland – he used the term in a speech in 1939 at the American Sociological Society.[4] He was a sociologist, who 80 years ago was upset that companies - businesses that were committing criminal acts were not being sufficiently prosecuted.[5]

Now, corporate criminal liability dates back prior to Sutherland's coining this phrase as seen in the case of *New York Central & Hudson River Railroad Co. v. United States*,[6] a case in which the Supreme Court allowed the government to prosecute a corporation for a crime violating the Elkins Act.[7] The statute required a *mens rea*, thus requiring an intent. Prior to this case, many said you could not prosecute corporations because, after all, how could a corporation have an intent when it had no mind; and how could a corporation act when it was a fictitious body, and further you can't put a corporation in prison. But the *New York Central* changed things – it said you could prosecute corporations even when the statute was not strict liability and even when the statute required a *mens rea*.

So corporate criminality existed, but Edwin Sutherland wanted more – he wanted *real enforcement* when these crimes were being committed by the corporations or the

---

[4] Reprinted in Edwin H. Sutherland, White-Collar Criminality, 5 Am. Soc. Rev. 1 (1940); *see also* ELLEN S. PODGOR, PETER J. HENNING, JEROLD H. ISRAEL & NANCY J. KING, WHITE COLLAR CRIME 2d Ed. 1-2 (2018)
[5] EDWIN H. SUTHERLAND, WHITE COLLAR CRIME: THE UNCUT VERSION 7 (1983).
[6] 212 U.S. 481 (1909).
[7] 22 Stat. at 847, chap. 708, U.S. Comp. Stat. Supp. 1907, p. 880.

individuals within them. He was a sociologist, and his emphasis was on the white collar. He wanted prosecution of crimes that were "committed by a person of respectability and high social status in the course of his occupation."[8]

Over time that definition changed with the emphasis moving to looking at the crime itself to determine if it was a white collar crime. There was less focus on the person committing the crime having a white collar, and more emphasis on whether the person worked in a corporation or business. The definition that was developed by Herbert Edelhertz looked at the offense as opposed to the offender.[9] The Department of Justice, FBI definitions, and the American Bar Association moved to definitions that looked at whether it was an economic non-violent crime.[10] And although white collar crime is not really statistically reported as a criminal law category, it tends to have within its realm, crimes involving fraud, Ponzi schemes, corruption, environmental offenses, financial crimes, and other types of non-violent economic crimes.[11]

Sometimes these crimes will also be reported separately – for example, the category of fraud is different from the antitrust category and the environmental crime category. But you'll find cases in each of these areas in both the sociological and legal textbooks and casebooks. Bottom line – the statistical reporting of white collar crime is fuzzy and the crimes included within it are even more problematic.

Professor Lucian Dervan and I wrote an article a few years back called *White Collar Crime: Still Hazy After All These Years* – and in this article we showed how RICO, the Racketeered Influenced and Corrupt Organization Act, includes mail fraud and wire fraud as two possible predicate acts for charging a RICO offense. But RICO also includes predicate acts such as murder. We, therefore, questioned whether RICO should be reported with white collar crime statistics.[12]

White collar crime does not have that magic criteria for its reporting and you will find DOJ and other statistical reporting sites with differing results. One may say white collar prosecutions went up last year, and the other may claim that it went down.

And yes, some statistics will report identity theft as a white collar crime and include credit card theft in that category because stealing the card's information is a form of identity theft.

What may seem like an academic monologue can, however, be important. How you categorize something can make a difference when it comes to funding. Different Attorney Generals have their priorities because they can't focus on everything, and have

---

[8] SUTHERLAND, *supra* note 5 at 7.
[9] *See* Herbert Edelhertz, *The Nature, Impact and Prosecution of White Collar Crime* 3, 12 (1970).
[10] *See* Podgor, et al, *supra* note 4 at 2-4.
[11] *See* Lucian E. Dervan & Ellen S. Podgor, *"White Collar Crime": Still Hazy After All These Years*, 50 GEO. L. REV. 709 (2016).
[12] *Id.*

to pick out the important items of the time. They list their priorities and that is where the money goes. Sometimes cybercrime or identity theft will get listed as a priority.

So back to my credit card being hacked. It looks like we have some white collar criminality here – and whether it will be at the top of the priorities or bottom is something that can make a difference in how its enforced.

But now we have to look at the second question: who is doing the enforcement and who is paying the check for it?

The Identity Theft Resource Center's report[13] stated that the number of credit cards exposed in 2017 "totaled 14.2 million,[14] up 88% over 2016."[15] Data breaches may have played a role in the increase in credit card fraud and there have been many data breaches recently.[16] The Identity Theft Resource Center reported 791 data breaches.[17] I emphasize here the word "reported," as many companies do not report when they experience a data breach. In the United States by the end of June 2017, there was a 29% increase over the same period in 2016 of reported data breaches, the highest number reported for any half year period.[18]

So, although in-person credit card theft is down, because companies are doing things like using EMV chips,[19] online credit card fraud is up.[20] Today, many of us order items online, we pay for these items online, and we do many transactions online. Javelin Strategy and Research reported that in 2017 there was 16.7 million victims of identity theft and $16.8 billion was stolen.[21]

But when my credit card was compromised, I did not pay anything beyond the charges that I had made. Others, however, did pay for this criminal activity. The Consumer Sentinel Network maintained by the Federal Trade Commission (FTC) said there were

---

[13] IDENTITY THEFT RES. CTR., *2017 Annual Data Breach Year-End Review* (2018), *available at* https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last visited April 22, 2019); *see also* Experian, *Identity Theft Statistics*, *available at* https://www.experian.com/blogs/ask-experian/identity-theft-statistics/ (last visited April 22, 2019).
[14] IDENTITY THEFT RES. CTR., *Data Breaches Up Nearly 45 Percent* (last visited Mar. 21, 2019), https://www.idtheftcenter.org/data-breaches-up-nearly-45-percent-according-to-annual-review-by-identity-theft-resource-center-and-cyberscout.
[15] IDENTITY THEFT RES. CTR., *supra* note 13.
[16] *Id.*
[17] IDENTITY THEFT RES. CTR., *2017 Data Breaches Hit Half-Year Record High* (last visited Mar. 21, 2019), https://www.idtheftcenter.org/2017-data-breaches-hit-half-year-record-high.
[18] *Id.*
[19] VISA, *Chip Technology Helped Reduce Card-Present Counterfeit Payment Fraud* (last visited Mar. 21, 2019), https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html.
[20] INS. INFO. INST., *Facts+Statistics: Identity Theft and Cybercrime* (last visited Mar. 21, 2019), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.
[21] *Id.*

2.7 million identity theft and fraud reports received in 2017, and it cost "consumers almost $905 million" for an average of $429 per consumer.[22] Overall, credit card fraud was the "most reported" in all these reports.[23] Consumers do suffer in that they may suffer the lost time, missing work, having to temporarily borrow money, and the aggravation of straightening out their credit reports. All of this is a nuisance, and even more so if the individual has their entire identity stolen.

Typically, it is the banks and/or credit card companies that bear the burden when there is credit card fraud. Banks often issuing the credit cards are the first in line to feel the sting of credit card fraud.[24] Second, the burden can be on the corporation or business that is selling the goods. If the business is Target, Amazon, or a major company, they may factor these losses into their prices, and if the business is a bank, they factor this into the seller's costs.[25] But if you are a small business, credit card losses can really set you back.[26]

There are additional costs to businesses and companies, as they have to make certain that they have appropriate security so that the thieves do not get into their technology systems. They may also be saddled with the costs of litigation,[27] as lawsuits and attorney fee costs between banks and companies may need to be factored into funds being expended.[28] Major credit card companies sometimes put costs on the small banks,[29] which can be devastating when there is a huge fraud breach. Costs can include notifying customers of the company of the data breach, as well as the business losses faced when the customer no longer trusts the company.[30] The dollars can just keep adding up when there is a fraud or breach. Financial institutions and companies probably get hit the hardest in paying the check for damage from these illegal activities.

---

[22] *Id.*

[23] *Id.* They note that it "was the most reported incident to the Consumer Sentinel Network, with 133,000 reports." *Id.*

[24] Lindsey Konsko, *Who Pays When Merchants Are Victims of Credit Card Fraud?*, NERDWALLET (June 3, 2014), https://www.nerdwallet.com/blog/credit-cards/merchants-victims-credit-card-fraud.

[25] *Id.*

[26] *Id.*; *see also* C.T. CORP.., *Business Identity Theft is a Big Threat to Small Business* (Oct. 11, 2018), https://ct.wolterskluwer.com/resource-center/articles/business-identity-theft-small-business-threats (considerations for small business owners to contemplate in thwarting identity thieves).

[27] INS. INFO. INST., *supra* note 8; *see also* GENERALI GLOB. ASSISTANCE & IDENTITY THEFT RES. CTR., *The Impact of Cybersecurity Incidents on Financial Institutions* (2018) (retrievable at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf).

[28] Konsko, *supra* note 24.

[29] *Id.*

[30] GENERALI GLOB. ASSISTANCE & IDENTITY THEFT RES. CTR., *supra* note 16.

Corporations and banks do not get much sympathy these days. On one hand, fraud by entities has been receiving increased exposure.[31] We see corporate executives being called before Congress to testify concerning fraudulent conduct within their companies. One cannot justify the conduct of bank employees creating fake accounts.[32] So, on one hand there are fraud and abuses occurring within companies, but there may also be abuses by others outside the entity which fall upon them. This is because companies and financial institutions bear the cost of enforcement in different ways.

First, we see companies bearing huge compliance costs, as they cannot survive in today's world absent compliance programs - programs that will assure that fraud and other crimes are not occurring internally within the entity. Those on the board of directors have the added responsibility under the *Caremark* case[33] to make certain that the company has such a compliance program. Compliance programs provide oversight to assure that a rogue employee within the company will not be doing something harmful to the company; and if they do, then the compliance officers will catch it immediately. But it is the corporation, not the government, that pays the costs of enforcing these compliance programs.

Second, companies also have exposure when something potentially illegal occurs within the company. They may be hiring outside counsel to conduct an internal investigation.

Third, in addition to doing an internal investigation, they may also find themselves getting a deferred prosecution agreement (DPA) or a non-prosecution agreement (NPA), which might have the additional cost of hiring a monitor. Monitors can be costly, with some of these fees being the subject of controversy.[34]

And fourth, if company employees are alleged to be part of the fraud, the company may be hiring attorneys to represent them. This might result from the employee-employer employment agreement, or it may be simply an attempt by the company to keep control of the case. But the corporation may be wanting to pay corporate executive's attorney fees or they may have to pay these attorney fees under an employment contract.[35]

---

[31] R. Robin McDonald, *Judge OKs Equifax Lawsuits Over Massive Data Breach,* NAT'L LAW JOURNAL (Jan. 28, 2019), https://www.law.com/dailyreportonline/2019/01/28/judge-oks-equifax-lawsuit-over-massive-data-breach.

[32] Garrett Pelican, *Former Citibank Employee Pleads Guilty to Fraud After Stealing from Customers*, FLA. TIMES-UNION (Jan. 27, 2017, 6:01 PM), https://www.jacksonville.com/news/2017-01-27/former-citibank-employee-pleads-guilty-fraud-after-stealing-customers

[33] *See* In re Caremark Int'l Inc. Deriv. Litig., 698 A.2d 959 (Del. Ch. 1996).

[34] Philip Shenon, *Ashcroft Deal Brings Scrutiny in Justice Dept.*, N.Y. TIMES, Jan. 10, 2008 (noting fees of greater than 28 million dollars).

[35] *See* United States v. Stein, 541 F.3d 130 (2d Cir. 2008)(finding that the government cannot interfere with attorney fees being paid by an accounting company to its employees).

Financial industries also may be paying costs that assist law enforcement. For example, in the case of *Bank of New England,*[36] the court found that you can use "collective knowledge" to obtain the *mens rea* for entity liability. A company may have different pieces of the intent in different parts of the company, something that is especially true in larger companies. The government can put all the pieces together to obtain "collective knowledge" to have a sufficient *mens rea*.

But what really happened in the *Bank of New England* case was that the government was implementing the first ever case against a bank for failure to properly file Currency Transactions Reports—"CTRs"—when accepting over ten thousand dollars in cash from a customer. Congress required this of banks when they passed the Bank Secrecy Act in 1970.[37] But the impetus behind these actions was to eradicate drugs. Having banks fill out CTR forms was a way for the government to monitor and ascertain money laundering and drug trafficking. Recognizing that drugs and money laundering were infiltrating society, law enforcement could secure needed information to assist them through monitoring money flowing through banks.[38] This came at a cost to the banks as it required them to have sufficient computerization to monitor the inflow of bank funds in a time when computerization was first coming on the scene. It also required banks to have sufficient personnel to fill out the needed CTR forms. Banks needed to have training within the financial institutions to make certain that the bank tellers knew what to ask and how to properly fill out the CTR forms. It also required the financial institutions to have mechanisms to make certain that there was appropriate compliance in banks. The costs here were borne by the financial institutions.

So, it may be a nuisance to a consumer when their credit card is hacked. It may cause one to focus more closely on their credit cards and statements. But the cost is minimal in comparison to what is being paid by companies and financial institutions. Maybe the cost of products sold to consumers by the companies will go up in price, or maybe the cost of bank fees will rise. But, the main parties to bear the costs will be companies, financial institutions, and insurance companies insuring these expenses.

It may seem odd to be defending companies and financial institutions today, when they are often the ones who have allegations against them for fraudulent conduct. But when 46% of Americans are having their credit cards compromised and the number is increasing,[39] perhaps we need to focus also on putting a stop to this criminal activity.

We need to recognize that the crime of the past is not the crime of today or tomorrow. The check for this criminal activity should not be borne exclusively by companies and

---

[36] *See* United States v. Bank of New England, N.A., 821 F.2d 844 (1st Cir. 1987).
[37] 31 U.S.C.A. § 5311.
[38] 31 U.S.C.A. § 5313.
[39] Rebecca Lake, *23 Frightening Credit Card Fraud Statistics*, CREDIT DONKEY (last visited Mar. 22, 2019), https://creditdonkey.com/credit-card-fraud-statistics.html.

financial institutions. This criminal activity needs to be prioritized by the Department of Justice (DOJ).

Do not get me wrong—DOJ is already doing some prosecutions in this area. Recent DOJ press releases include: "*Federal Jury Convicts Twin Brothers for Credit Card Fraud and Identity Theft in Gas Pumping Cases;*"[40] "*Final Defendant in $3.1 Million Credit Card Scheme Sentenced*;"[41] and "*Former Citibank Employee Pleads Guilty to Credit Card Fraud.*"[42]

There was a recent study done by the United States Sentencing Commission[43] on mandatory minimums on identity theft offenses that demonstrated that offenders convicted of § 1028A,[44] (Aggravated Identity Theft), comprised only 1.6% of federal offenders for 2016.[45] And yet § 1028A offenses accounted for 7.2% of the offenses carrying the mandatory minimum penalty.[46] And 53.4% of identity theft cases had convictions under § 1028A.[47] This demonstrates that Congress has done its job in increasing penalties for these offenses. It is true that some companies may not be quick to turn over massive breaches of information to the DOJ for them to investigate and prosecute,[48] as this does not provide a positive picture for a company. But perhaps these companies will be more likely to cooperate with the DOJ if they knew that the government would pick up more of the check on prosecuting more of these cases.

We as citizens also need to do more. As former President John F. Kennedy said, "Ask not what your country can do for you, but what you can do for your country."[49] So in honor

---

[40] Press Release, U.S. Dep't of Justice, Federal Jury Convicts Twin Brothers for Credit Fraud (Apr. 25, 2018), https://www.justice.gov/usao-mdfl/pr/federal-jury-convicts-twin-brothers-credit-card-fraud-and-identity-theft-gas-pump.

[41] Press Release, U.S. Dep't of Justice, Final Defendant in $3.1 Million Credit Card Fraud Scheme Sentenced (Oct. 26, 2016), https://www.justice.gov/usao-sdoh/pr/final-defendant-31-million-credit-card-fraud-scheme-sentenced.

[42] Press Release, U.S. Dep't of Justice, Former Citibank Employee Pleads Guilty to Credit Card Fraud (Jan. 27, 2017), https://www.justice.gov/usao-mdfl/pr/former-citibank-employee-pleads-guilty-credit-card-fraud.

[43] U.S. SENTENCING COMM'N: MANDATORY MINIMUM PENALTIES FOR IDENTITY THEFT OFFENSES (Sept. 2018) [hereinafter MANDATORY MINIMUM REPORT] (retrievable at https://www.ussc.gov/research/research-reports/mandatory-minimum-penalties-federal-identity-theft-offenses).

[44] 18 U.S.C. § 1028A.

[45] MANDATORY MINIMUM REPORT at 4.

[46] *Id.*

[47] *Id.*

[48] Nir Kossovsky, *Insight: DOJ Policy to "Flip" Corporate Defendants Catches Eye of D & O Underwriters*, Bloomberg Law, January 9, 2019, *available at* https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-doj-policy-to-flip-corporate-defendants-catches-eye-of-d-o-underwriters (last visited April 29, 2019).

[49] John F. Kennedy, Inaugural Address (Jan. 21, 1961).

of Identity Theft month,[50] we need to assist by checking our credit card statements regularly; responding promptly when a credit card company notifies us that there might be a fraud on our card, and setting up extra security, like multi-factor authentication and rotating passwords.[51] Being alert to our financial transactions is an important step to curbing credit card fraud. We have learned to become alert in our airports, on trains, and in schools. But we also need to be alert online.

Many speak or write today about fraud within the company - whether it be a corrupt individual, or fraudulent activity within a corporation. The focus is often on who should be prosecuted, the value of lack thereof of the Yates Memo,[52] and the divisive nature of the current corporate and business environment. Let us also not forget that corporations have enormous pressures being placed upon them, one of which is how to handle online fraudulent conduct. This is white collar crime and it needs to be a government priority. Thank you very much.

---

[50] Am. Bankers Ass'n., *2019 Consumer Awareness Observances* (last visited Mar. 22, 2019), https://www.aba.com/Press/Documents/ConsumerAwarenessObservancesCalendar.pdf.

[51] Cassy Perera, *23 Ways to Prevent Identity Theft*, CREDIT DONKEY (last visited Mar. 22, 2019), https://www.creditdonkey.com/prevent-identity-theft.html.

[52] *See generally* John C. Richter, Brandt Leibe & William S. McClintock, *INSIGHT: Individuals Remain Focus After D.O.J. Revisions to Yates Memo on Individual Accountability*, BLOOMBERG LAW (Jan. 24, 2019 4:00 AM), https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-individuals-remain-focus-after-doj-revisions-to-yates-memo-on-individual-accountability.