Northwestern Journal of Technology and Intellectual Property

Volume 16 | Issue 2 Article 2

2018

"CAN I GET YOUR DIGITS?": ILLEGAL ACQUISITION OF WIRELESS PHONE NUMBERS FOR SIM-SWAP ATTACKS AND WIRELESS PROVIDER LIABILITY

Nathanael Andrews
Northwestern Pritzker School of Law, Northwestern University

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

"CAN I GET YOUR DIGITS?": ILLEGAL ACQUISITION OF WIRELESS PHONE NUMBERS FOR SIM-SWAP ATTACKS AND WIRELESS PROVIDER LIABILITY

Nathanael Andrews

November 2018 VOL. 16, NO. 2

Volume 16, Number 2 (2018)
Northwestern Journal of Technology and Intellectual Property

Notes

"CAN I GET YOUR DIGITS?": ILLEGAL ACQUISITION OF WIRELESS PHONE NUMBERS FOR SIM-SWAP ATTACKS AND WIRELESS PROVIDER LIABILITY

Nathanael Andrews[1]

ABSTRACT—In a SIM-swap attack, a hacker uses text messages sent to a wireless customer's phone number to reset passwords and access critical accounts. These SIM-swap attacks are often targeted at cryptocurrency (e.g., bitcoin) holders and can result in thousands or even millions of dollars in losses. Wireless providers are often the weakest point exploited by hackers in SIM-swap attacks. These hacks are even more insidious because they rely primarily on social vulnerabilities rather than technical skill: hackers pressure accommodating customer service agents or bribe wireless provider employees in order to gain control of a wireless providers account and phone number. The wireless account and phone number provide a gateway to all the wireless customer's digital accounts through password reset codes sent to the victim's phone number, which is controlled by the hacker. Yet, wireless providers have failed to protect this gateway. Experience has shown that it is surprisingly too easy for a hacker to gain control of a wireless customer's phone number. This note argues that wireless providers should be liable for negligence according to a reasonableness standard of care. Such a standard would motivate them to do more to protect wireless customers.

Wireless customers are being harmed by hackers. Wireless providers are positioned to prevent that harm by blocking unauthorized control of customer phone numbers. This note provides background on the SIM-swap attack, addresses policy arguments supporting the liability of wireless providers, examines how liability of wireless providers can be found under statutory federal law, and argues that common law negligence is the most appropriate route to wireless provider liability. The policy-based arguments address victims with a pressing need for remedy, wireless providers as the least cost avoider, and wireless providers as the most competent avoider. The

[1] J.D. Candidate, Northwestern Pritzker School of Law, 2019.

law-based arguments address the roles of the FCC and the FTC in SIM-swap attacks and distinguish developments in negligence common law liability for general data breaches. In short, this note argues that SIM-swap attacks give rise to important harms, wireless providers should be liable for those harms, and negligence with a reasonableness standard of care is the right standard for liability.

I. INTRODUCTION

Thieves are stealing millions of dollars from wireless customers thousands of times each month.[2] The mechanism of theft is known as a SIM-swap attack: a thief gains unauthorized control of a wireless customer's phone number to use SMS-based text messages to reset the wireless customer's passwords and steal valuable assets from critical accounts. This note argues that wireless providers can and should do more to prevent these types of hacks.

Frequent massive data breaches of major consumer-facing companies have left the population at large wondering about the ways in which they have been injured and who is responsible. As such, much attention and analysis has been devoted to data breach liability and related issues. This note addresses a similar issue, SIM-swap attacks, arising from a similar type of event; however, the nature of SIM-swap attacks is fundamentally different from data breaches in two key ways. First, SIM-swap attacks are targeted attacks on individuals. This contrasts with the large groups affected by most data breaches. Second, SIM-swap attacks often result in theft of digital assets, such as bitcoin, that have substantial, quantifiable financial value. This contrasts with the more difficult to quantify and intangible harms of privacy violations and increased risk of identity theft associated with most large-scale data breaches.

These two fundamental differences between SIM-swap attacks and more typical data breaches help to frame the discussion in this note and highlight the importance of giving SIM-swap attacks special attention. The first difference, that fewer people are affected, emphasizes that targeted SIM-swap attacks will naturally receive less overall attention from law enforcement and public regulators.[3] When coupled with the second difference, that victims are tangibly and substantially harmed, this leads to the potential problem that a lesser number of people will suffer a greater harm without being able to generate enough interest to facilitate a solution.

At the same time, these two fundamental differences gravitate towards an elegant and attainable solution: place the liability on the party best situated to prevent the harm, the wireless provider. Assigning liability to wireless providers is an elegant solution because the damages are easy to determine—

---

[2] Nathaniel Popper, *Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency*, N.Y. TIMES (Aug. 21, 2017), https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html [https://perma.cc/R9WT-UWPL].

[3] However, the number of victims continues to grow, and media attention has increasingly highlighted these often devastating hacks. *See, e.g.*, Lorenzo Franceschi-Bicchierai, *The SIM Hijackers*, MOTHERBOARD (July 17, 2018, 8:33 AM), https://motherboard.vice.com/en_us/article/vbqax3/hackers-sim-swapping-steal-phone-numbers-instagram-bitcoin [https://perma.cc/2BTY-DHM7].

they are simply the cost to be made whole by recovering the stolen digital assets—and because the limited number of SIM-swap victims, relative to data breaches with millions of victims, protects wireless providers from unlimited liability. Wireless providers are also the least cost avoider, as many SIM-swap attacks can be traced to weak security practices by the carriers or unfaithful employees.

Wireless customers are being harmed by hackers. Wireless providers are positioned to prevent that harm. This note argues that wireless providers should be and are liable for failing to prevent unauthorized control of wireless customer phone numbers. The discussion proceeds in three main parts. Following this introduction, Part II provides background on the underlying problem itself, the SIM-swap attack. Part III argues that strong policy factors dictate that liability *should* be assigned to wireless providers. Part IV argues that liability may be attached to wireless providers under current federal laws, but the common law negligence duty of care is the best route for wireless provider liability. Structured in these three parts, this note argues that wireless providers should be liable for SIM-swap attacks by explaining why SIM-swap attacks are important, why wireless providers should be liable, and how liability should be structured.

II. PROBLEM BACKGROUND

A. Cybersecurity in a nutshell: what are the keys and who has them?

Concurrent with locking anything important is the consideration of controlling access to the key. From online banking to social media, consumer cybersecurity is—in a simplistic sense—no different: digital accounts have keys granting access and controlling access to those keys is fundamental to account security. Keys distinguish between authorized and unauthorized access to digital accounts. Passwords generally serve as these keys. The account owner and account provider are theoretically the only ones who have the passwords. However, user passwords are an awful mess.

B. The problems with passwords: passwords are easy to guess and easy to forget

There are two dominant problems with passwords.[4] First, user passwords are often "weak" or easy to guess.[5] Many passwords include exclusively or as a part "123," "123456," "asdf," "password," birthdays, pet names (undoubtedly posted on Facebook), or other staggeringly obvious

[4] Daniel J. Solove & Woodrow Hartzog, *Should the FTC Kill the Password? The Case for Better Authentication*, 14 PRIVACY & SEC. L. REP. (BNA) 1353, 2–3 (2015).

[5] *Id.* at 3–4.

features.[6] Second, despite being weak or easy to guess, passwords are often forgotten.[7] Thus, improving the keys securing our information, content, and assets must move beyond the password.[8]

C. A briefly brilliant solution: two-factor authentication

Two-factor (or multi-factor) authentication was developed to address the two main problems with passwords. Two-factor authentication account keys incorporate two elements (or factors): (1) the user password and (2) a variable code the user can access.[9] Cell phone apps and text messages are common sources of the variable code. For text message (or SMS) based two-factor authentication, the account provider sends the variable code directly to the account holder's cell phone by text message.[10] To access her account in such a system, the user must enter both her password and a code sent by text message.[11] These text codes also enable a user to reset her password if she forgets it.[12] Thus, SMS-based two-factor authentication apparently addresses both drawbacks of standalone passwords for user accounts: improving security and resetting forgotten passwords.

D. Vulnerabilities: technical hacking and social hacking

Unfortunately, this seemingly brilliant solution has a serious vulnerability. SMS-based two-factor authentication depends on the user controlling her phone number. Although the code delivered by text message improves security and aids password reset, a potential hacker can use password reset to gain unauthorized account access if the hacker can gain control over the user's phone number. This vulnerability is exploited using

---

[6] *Id*.

[7] *Id*.

[8] *Id*. at 5–7.

[9] *Id*. at 4; Tom Mighell, *Protecting Your Online World with Two-Factor Authentication*, 41 No. 2 L. Prac., 32, 32 (2015); Paul Rice, *Civil Liability Theories for Insufficient Security Authentication in Online Banking*, 10 DEPAUL BUS. & COMM. L.J. 439, 445–47 (2012).

[10] Mighell, *supra* note 9, at 32. Cell phone apps, though not primarily addressed herein, provide a more secure method where the code is not sent to the account holder. *Id*. Instead, the account holder has an app on her cell phone that generates the code using a cryptographically secure method based on a secret seed code that the account provider also has access to. *Id.* Many services do not support this type of security mechanism and instead rely exclusively on SMS-based two-factor authentication. Russell Brandom, *Two-factor Authentication Is a Mess*, VERGE (Jul. 10, 2017, 9:26 AM), https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess [https://perma.cc/9WR4-M7FA].

[11] Mighell, *supra* note 9, at 32.

[12] Thomas Brewster, *All That's Needed to Hack Gmail And Rob Bitcoin: A Name and a Phone Number*, FORBES (Sept. 18, 2017, 9:00 AM), https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/#73dde70e41a4 [https://perma.cc/56ZU-GQHN].

two techniques.[13] The first technique is a *technical* approach involving vulnerabilities in the SMS system to intercept text messages.[14] For this technique, hackers exploit weaknesses in an interoperability standard used by telecommunications companies, referred to as Signaling System No. 7 (SS7), to directly intercept messages transmitted using the interoperability standard.[15] Though a real vulnerability, it requires a high level of sophistication to exploit. The second technique is a *social* approach involving vulnerabilities in wireless provider procedures governing phone number transfers.[16] This technique is known as a SIM-swap attack. Because the primary vulnerability is *social* in nature, the SIM-swap attack is more insidious in that it is not a sophisticated attack. Instead, SIM-swap attacks require only accommodating customer service agents—or bribable wireless provider employees—and persistent, persuasive hackers willing to pressure accommodating customer service agents or bribe wireless provider employees.[17]

E. Anatomy of a SIM-swap attack

A SIM-swap attack begins with the hacker obtaining the user's phone number, which is often found online with basic research.[18] Then the hacker calls the wireless provider and asks to transfer the phone number to a new

---

[13] PAUL A. GRASSI ET AL., NIST SPECIAL PUBLICATION 800-63B, DIGITAL IDENTITY GUIDELINES: AUTHENTICATION AND LIFECYCLE MANAGEMENT, § 8 (2017); Laura Shin, *Hackers Have Stolen Millions of Dollars in Bitcoin -- Using Only Phone Numbers*, FORBES (Dec. 20, 2016, 1:59 PM), https://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#689e9f5738ba [https://perma.cc/2ARZ-5HUB]; Russell Brandom, *This Is Why You Shouldn't Use Texts for Two-Factor Authentication*, VERGE (Sept. 18, 2017, 1:17 PM), https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin [https://perma.cc/2MSN-BTM7]; Dan Goodin, *Thieves Drain 2fa-protected Bank Accounts by Abusing SS7 Routing Protocol*, ARS TECHNICA (May 3, 2017, 2:40 PM), https://arstechnica.com/information-technology/2017/05/thieves-drain-2fa-protected-bank-accounts-by-abusing-ss7-routing-protocol/ [https://perma.cc/VV64-GVNX]; Brewster, *supra* note 12; Franceschi-Bicchierai, *supra* note 3; Popper, *supra* note 2.

[14] GRASSI ET AL., *supra* note 12, § 8; Brewster, *supra* note 12; Brandom, *supra* note 13; Goodin, *supra* note 13.

[15] Goodin, *supra* note 13.

[16] COLLIN MULLINER ET AL., *SMS-Based One-Time Passwords: Attacks and Defense*, TECH. UNIV. OF BERLIN TECH. REPORT 2014-02, 1, 5 (2014); GRASSI ET AL., *supra* note 12, § 8; Shin, *supra* note 13.

[17] Franceschi-Bicchierai, *supra* note 3. Further developments uncovered by the press exposed the common practice of bribing wireless provider employees during a SIM-swap attack to get around a user's account password using an employee's credentials. *See* Colin Lecher, *Florida Man Arrested in Alleged Multi-state SIM Card Hacking Ring*, VERGE (Aug. 11, 2018, 11:00 AM), https://www.theverge.com/2018/8/11/17671698/sim-card-fraud-arrest-florida-cyber-fraud [https://perma.cc/5Z43-ND7X].

[18] Russell Brandom, *Anatomy of a Hack*, VERGE (Mar. 4, 2015), https://www.theverge.com/a/anatomy-of-a-hack [https://perma.cc/RC66-R8NS].

device, such as a cheap cell phone, with a new SIM card.[19] Although the wireless provider may require some type of password to transfer the phone number, the password can be bypassed by the customer service agent.[20] Thus, a persuasive, angry, or persistent hacker can convince the customer service agent to transfer the phone number. Alternatively, some hackers simply bribe wireless provider employees to obtain or bypass a user's account password.[21] As soon as the phone number is transferred to the hacker's SIM-card, the hacker begins resetting passwords on the user's various digital accounts using text message codes.[22] Then, account by account, usually starting with e-mail, the hacker gains control of the user's information, content, and assets.[23] The SIM-swap attack is not technically sophisticated; it only requires persuasion, anger, persistence, or some combination thereof—or an unscrupulous employee.

F. The damage done by SIM-swap attacks is large and growing

SIM-swap hacks have stolen millions of dollars.[24] Although replacing SMS-based two-factor authentication is likely best in the long term, the practical issue is that numerous accounts use SMS-based two-factor authentication today. Even more troubling, these SIM-swap attacks are on the rise, more than doubling from 2013 to 2016 with over 2,500 such attacks being reported in January 2016.[25] Indeed, the media has responded to this rise by raising the alarm, exemplified in articles by Thomas Brewster, Laura Shin, Russell Brandom, and Nathaniel Popper.[26] Law enforcement has also responded by pursuing some of the perpetrators.[27] The damage due to SIM-swap attacks is rising and the frequency is increasing. And the burden of that damage on an individual can be large, with one lawsuit alleging losses of $24 million.[28]

A better solution may come in the future. But for today, the poor user—who has $10,000 (or more) of bitcoins stolen, has her Twitter account

---

[19] *Id.*

[20] *Id.*

[21] Franceschi-Bicchierai, *supra* note 3.

[22] Brandom, *supra* note 18.

[23] *Id.*

[24] Popper, *supra* note 2. At least two lawsuits have been filed against wireless providers for SIM-swap attacks. Complaint, Tapang v. T-Mobile USA, Inc., No. 2:18-cv-00167 (W.D. Wash., Feb. 4, 2018) [hereinafter *Tapang Complaint*]; Complaint, Terpin v. AT&T Inc., No. 2:18-cv-06975 (C.D. Cal., Aug. 15, 2018) [hereinafter *Terpin Complaint*].

[25] Popper, *supra* note 2.

[26] Brandom, *supra* note 13; Brewster, *supra* note 12; Popper, *supra* note 2; Shin, *supra* note 13.

[27] Lecher, *supra* note 17.

[28] *Terpin Complaint*, *supra* note 24, ¶ 108.

controlled by a gloating fifteen-year-old hacker, and has lost all the personal information in her e-mail to the same fifteen-year-old—is left thinking, "Why did my wireless provider transfer my phone number to this hacker?" The keys to digital accounts, containing personal information, content, and assets, are accessible via phone numbers. Thus, phone numbers have become in themselves the digital keys to the kingdom that unlock access to users' digital and real lives. Wireless providers should not be free to give users' keys away.

III. POLICY-BASED ARGUMENTS: WIRELESS PROVIDERS *SHOULD* BE LIABLE FOR UNAUTHORIZED ACCOUNT ACCESS AND SIM-SWAP ATTACKS BECAUSE WIRELESS PROVIDERS ARE BOTH THE LEAST COST AVOIDER AND THE MOST COMPETENT AVOIDER

A. Liability should be assigned because damages and causation demonstrate a pressing need

The injury to the wireless customer in a SIM-swap attack is substantial. Further, the causal link is clearer for SIM-swap attacks than for general data breaches. Unlike general data breaches, where injury to the customer is not immediate and causation is difficult to find, SIM-swap attacks cause tangible injury to the wireless customer and causation is easy to find. This section justifies the need to assign liability by presenting the substantial injuries suffered by the wireless customer and the causal link to the SIM-swap attack.[29]

As in data breaches, SIM-swap attacks can create several types of victims. However, unlike in data breaches, the customer is harmed much more by the SIM-swap attack than the company. The wireless provider may cease receiving customer account payments due to a SIM-swap attack. In contrast, the wireless customer loses control of her phone number, access to multiple digital accounts, and thousands or even millions of dollars.[30] Thus, unlike major data breaches of personal information or credit card information seen in heavily publicized breaches at, e.g., Yahoo!, Target, Home Depot, and Equifax, individually targeted SIM-swap attacks place a much greater share of the injury on the individual wireless customer.

---

[29] This section focuses on identifying the party most competent to prevent SIM-swap attacks. Thus, the individual account providers for each account breached using the compromised wireless phone number, such as Gmail or Dropbox, for example, are largely ignored because these accounts are not the route of the SIM-swap attack. The role and liability of the individual account providers is a critical issue that deserves much discussion, but for this note, the individual account providers are the ends and not the means of SIM-swap attacks.

[30] *See, e.g.*, Brandom, *supra* note 18; *see also Terpin Complaint*, *supra* note 24, ¶ 108.

In contrast to general data breaches, the large individual injuries of SIM-swap attacks present more cognizable injuries that legal decision makers cannot ignore. In SIM-swap attacks, wireless providers are generally not exposed to the substantial costs associated with major breaches. Instead, the attack is focused on a single customer of the wireless provider. Thus, the apparent cost to the wireless provider is the potential loss of a single customer.[31] Contrast that to the SIM-swap victim where the phone number is used to reset passwords of the victim's digital accounts in order to gain control of the victim's e-mail, social media, online banking accounts, financial transaction accounts (e.g., PayPal and Venmo), utilities, cloud storage, and cryptocurrencies.[32] When a thief gains control of each account on this list, there are two types of harm: massive privacy invasion and direct financial harm.

In the privacy category, control of many or all digital accounts goes beyond the increased risk of identity theft. In these scenarios a hacker has access to every e-mail the victim has written, every post and private message on social media, every file and picture backed up in the cloud, and even every text message backed up in the cloud.[33] As a worst-case scenario, the hacker could have access to transcripts of past relationships, medical records and diagnosis, records of every mistake the victim made, and inappropriate or scandalous pictures, video, or behaviors.[34] Although often ignored by legal decision makers as intangible, these are deep privacy violations with the potential to ruin lives.[35]

---

[31] Contrast this with major data breaches that incur multiple costs including notifying the victims, obtaining thorough breach analysis, replacing compromised equipment and systems, increased regulatory compliance, fraud monitoring services for affected customers, and covering fraudulent charges in certain circumstances. Michael D. Simpson, *All Your Data Are Belong to Us: Consumer Data Breach Rights and Remedies in an Electronic Exchange Economy*, 87 U. COLO. L. REV. 669, 682–83 (2016). For example, in a credit card information breach, the credit card issuer may spend heavily replacing stolen cards and crediting fraudulent charges. Another potential major cost of breach is the loss of public confidence causing decreases in business and public investment. *Id.* In the aggregate, these various costs to the breached business are substantial.

[32] *See supra* Section II.E and II.F. Compare SIM-swap victim injuries with the costs for victims of general data breach, which are more speculative. Simpson, *supra* note 31, at 684–85. Costs to the customer might be increased threat of identity theft and time spent dealing with actual identity theft, fraudulent charges that are not always refunded by the financial institution, identity theft monitoring costs, or privacy intrusions that, though personally damaging, are not financial in nature. *Id.* The cost to the breached business is often considered to be large while the individual injuries are often considered to be small. This concept, justified or not, is likely one reason courts, legislatures, and regulatory agencies have not provided a clear path for individual redress following a major data breach. *See infra* Section IV.A.

[33] Brandom, *supra* note 18; Popper, *supra* note 2.

[34] *See, e.g.*, Adrianne Jeffries, *Photos Hurt*, VERGE (Sept. 3, 2014, 5:26 PM), https://www.theverge.com/2014/9/3/6103265/photos-hurt [https://perma.cc/G8AS-ZG5E].

[35] *See* Simpson, *supra* note 31, at 685–86. *See also* discussion *infra* in Section IV.B.

In the direct financial harm category, thefts from cryptocurrency accounts holding, e.g., Bitcoin or Ethereum present very appealing targets for SIM-swap attacks that translate into concrete and cognizable harm.[36] A cryptocurrency holder might take security seriously, enabling two-factor authentication and requiring multistep authorization through more than one e-mail account to transfer cryptocurrency from an account. However, because the hacker uses the SIM-swap attack to gain control of the phone number for two-factor password resets of even multiple e-mail accounts and the online cryptocurrency account, the cryptocurrency holder's extra security efforts are bypassed at the wireless provider through social hacking.[37] Cryptocurrency account holders may have substantial funds in these accounts, ranging into the millions of dollars.[38]

Cryptocurrency thefts present the type of tangible injury that legal decision makers should not ignore.[39] The cryptocurrency market capitalization is currently more than $200 billion.[40] A popular U.S. cryptocurrency exchange and account provider has over twenty million accounts and has transferred more than $150 billion in cryptocurrency assets.[41] SIM-swap attacks expose victims to theft of cryptocurrency with real, tangible, and substantial value. Making these victims whole requires replacing the stolen property, i.e., replacing the cryptocurrency assets.[42]

Further, problems with causation that plague general data breach negligence liability are not present with SIM-swap attacks. In negligence for data breach cases, courts have had trouble identifying harm and, especially, finding causation for such harm because the causal link between a user's

[36] *See supra* Section II.F. The risk of unauthorized access to online banking accounts and financial transaction accounts is also significant, but it is laid aside in this discussion because it has already been given substantial attention in the form of scholarship, legislative action, and banking procedures. Such substantial attention has translated into a higher likelihood of reimbursement for fraudulent charges. Further, the more mature and regulated banking industry produces a more robust financial paper trail that may give thieves pause.

[37] *See supra* Section II.D and II.E.

[38] There are multiple ways to hold cryptocurrency funds and online accounts are not required (which would limit the risk of theft of those funds via SIM-swap attack), but transferring and exchanging the funds is often done (in substantial volume) through online accounts with cryptocurrency exchanges. Thus, the danger of online account hacking is difficult to bypass.

[39] In a sense, the different legal decision makers have punted on individual victim injuries for general data breaches. By focusing on the lack of physical injury in typical data breaches, the victim is often prevented from seeking redress from liable parties. *See* discussion *infra* in Section IV.B.

[40] COINMARKETCAP, https://coinmarketcap.com/ (last visited Oct. 19, 2018) [https://perma.cc/4JDX-6FZS].

[41] COINBASE, https://www.coinbase.com/ (last visited Oct. 19, 2018) [https://perma.cc/H3Q5-PLS8].

[42] The hackers themselves are also liable for the illegal activity and theft; however, as in real theft, the thieves are often judgement-proof in civil court and the funds are never recovered from the thief even when the thief is caught. Simpson, *supra* note 31, at 685 n.108.

information being released in a data breach and that user's later identity theft or account hacking is very difficult to establish.[43] In contrast, a SIM-swap attack includes close temporal causation because the transfer of control over the phone number is immediately followed by password reset using that phone number and unauthorized access to other accounts, including cryptocurrency accounts where theft establishes clear damages.[44] Account password resets will generate evidence illustrating use of the illegally controlled phone number to reset account passwords, demonstrating the causal link. Thus, SIM-swap attacks include strong causal links to tangible cryptocurrency theft, which provides a straightforward assignment of liability for damages.

B. Wireless providers should be liable for SIM-swap attacks because wireless providers are the least cost avoider

Wireless providers are the least cost avoider in SIM-swap attacks. They are the gatekeepers controlling customer phone numbers, while customers have little ability to prevent SIM-swap attacks without wireless provider assistance. The cost would be minor for wireless providers to implement reasonable customer verification protocols before transferring phone numbers.

To assign liability for SIM-swap attacks, the costs of prevention for wireless providers must be weighed against the costs of prevention for wireless customers. Economic theory provides insight into the value of this weighing, instructing liability to be placed "on the party to a transaction who is the one that can fix the 'problem' while incurring the least cost."[45] In other words, put the cost on the least cost avoider.[46] In a market without failures or transaction costs, wireless providers and customers would agree to a price for better security.[47] However, because transaction costs cause issues such as information asymmetry and collective action problems, economic theory suggests placing liability on the least cost avoider.[48]

Identifying the least cost avoider involves, in a heavily abbreviated analysis, identifying an initial rough guess and applying three guidelines to

---

[43] *See infra* Section IV.B.

[44] Brandom, *supra* note 18; Popper, *supra* note 2.

[45] Paul Rosenzweig, *Cybersecurity and the Least Cost Avoider*, DAYZERO: CYBERSECURITY LAW AND POLICY (Nov. 5, 2013, 11:41 AM), https://lawfareblog.com/cybersecurity-and-least-cost-avoider [https://perma.cc/W7R2-MS6P]; *see also* R. H. Coase, *The Problem of Social Cost*, 56 J.L. & ECON. 837 (2013).

[46] Coase, *supra* note 45.

[47] *See, e.g.*, Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 313–14 (2006); Rosenzweig, *supra* note 45.

[48] *See, e.g.*, Hahn & Layne-Farrar, *supra* note 47, at 314–19; Rosenzweig, *supra* note 45.

refine and improve the selection.[49] The rough guess rules out cost bearers that "would *obviously* [convey] too great an expense" to reduce the targeted harm.[50] For example, accidents involving pedestrians likely could be sharply reduced if pedestrianism itself were substantially modified and limited, but the cost is likely too great because pedestrianism is "without ready substitution."[51] In other words, the cost should not be allocated such that a beneficial and valuable activity is essentially quenched.

With the rough guess made, three guidelines help clarify the least cost avoider.[52] The first guideline warns against expensive administrative costs.[53] If the cost to determine the least cost avoider is high, it may be better to assign an alternative cost avoider that is cheaper to identify even though the alternative cost avoider is more expensive.[54] The second guideline instructs that externalization of costs should be avoided.[55] One type of externalization that occurs is "due to inadequate knowledge," where a party that might be able to reduce the harmful activity lacks adequate knowledge to foresee and reduce the risk.[56] The third guideline suggests that costs should be placed on the party best able to transact or "bribe" others to reduce the harm.[57] This strategy encourages the market to correct allocation errors through use of the party with the cheapest transaction costs, i.e., the best briber.[58] These criteria guide the least cost avoider analysis for SIM-swap attacks.

SIM-swap attack avoidance costs intuitively weigh in favor of assigning the wireless provider as the least cost avoider as an initial rough guess.[59] Particular to SIM-swap attacks, the victims can do very little to avoid attacks without wireless provider assistance. Thus, the cost of avoiding SIM-swap attacks, if placed on victims, is likely a sharp reduction in use of digital accounts and assets that have value. But that implies too great a cost, just as quenching pedestrianism implies too great a cost, because digital accounts and assets are arguably of great economic benefit to society.[60] The customer can limit the potential injury by aggressively using other authentication

---

[49] GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 140–152 (Yale Univ. Press 2008) (1970).

[50] *Id.* at 140–41.

[51] *Id.*

[52] *Id.* at 143–52.

[53] *Id.* at 143–44.

[54] *Id.*

[55] *Id.* at 144–45.

[56] *Id.* at 148–49.

[57] *Id.* at 150–52.

[58] *Id.*

[59] *Id.* at 140–41.

[60] *Id.*

forms and avoiding SMS-based two-factor authentication. However, such steps are not always possible because many accounts only provide SMS-based two-factor authentication, and some require it.[61] Thus, unlike cases of consumer phishing, where the likelihood of injuries can be reduced by consumer carefulness, SIM-swap attacks are almost impossible to avoid by consumer vigilance, and the harm could only be diminished by avoiding beneficial activity altogether.[62] As a further distinction over phishing scams, which have been heavily publicized, SIM-swap victims suffer from lack of adequate knowledge. These victims lack knowledge of their vulnerability, because SIM-swap attacks are still underpublicized, as well as the know-how to adequately address their vulnerability.[63] That inadequate knowledge leads to externalization of the costs[64] in opposition to the second guideline.[65] Thus, the cost on each customer to avoid SIM-swap attacks is high and weighs against assigning liability.

On the other hand, the costs for the wireless provider of avoiding SIM-swap attacks are very reasonable, especially when divided across all customers served. The intuitive rough guess, the first guideline, and the third guideline all weigh in favor of wireless providers as the least cost avoider.[66] Specifically, wireless providers could increase the standards for authenticating access by requiring and enforcing account passwords other than the last four numbers of user Social Security Numbers, and this could be done without diminishing the overall usage of wireless services which would come at too great a cost to society.[67] Administratively—in accord with

---

[61] This point is also a key distinction from cases refusing to identify service providers as the least cost avoider. *See* Evra Corp. v. Swiss Bank Corp., 673 F.2d 951, 952–57 (7th Cir. 1982) (dismissing plaintiffs' negligence claim because plaintiff "showed a lack of prudence throughout" and the liability should be assigned to the party best "able to avert the consequence at least cost," which in this case did not immunize the plaintiff, as the customer, from liability because the court was able to identify multiple ways the plaintiff could have avoided the harm with prudent conduct). Unlike in *Evra Corp.*, where plaintiff could have avoided the harm with ordinary prudence, SIM-swap victims are powerless to avoid the harm of SIM-swap attacks without the wireless providers' assistance. *Id.*

[62] Jeremy Feigelson & Camille Calman, *Liability for the Costs of Phishing and Information Theft*, 13 J. INTERNET L. 1, 19–20 (2010).

[63] That said, media attention has been increasing and at least one high-profile lawsuit has been filed. *See supra* Section II.F noting articles covering SIM-swap attacks and the *Terpin Complaint*.

[64] The parties that will bear these externalized costs are likely the public, through deprivation of beneficial digital technology usage and advances, and the companies attempting to provide and maintain these digital accounts and assets, which will lose users who cannot prevent theft/breach.

[65] CALABRESI, *supra* note 49, at 144, 148–49.

[66] *Id*. at 140–53.

[67] *Id*. at 140–43. It appears that most carriers provide some option for increased security, but the level of compliance with the additional account security is unclear. *See, e.g.*, Lorrie Cranor, *Your Mobile Phone Account Could be Hijacked by an Identity Thief*, TECH@FTC (Jun. 7, 2016, 11:38 AM), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief [https://perma.cc/7XMM-VUCY].

the first guideline—it is cheaper to determine if the small number of wireless providers are implementing reasonable security for account access than to investigate every other point in the chain that may or may not be related to enabling SIM-swap attacks.[68] Requiring different passwords may involve additional training and infrastructure modification, but the fundamental process of phone number porting would remain unchanged as different passwords can be directly integrated with current systems. Further, if wireless providers are not the least cost avoider, they are nonetheless "the best briber" because they do not face coercion and collective action problems and they transact cheaply with customers due to their sophisticated business infrastructure.[69] Thus, the cost to wireless providers of requiring different passwords is small, especially when divided across all customers, and can be cheaply shifted in part to others.

Requiring different passwords and enforcing the password requirement without easy bypass by customer service will aggressively limit the effectiveness of SIM-swap attacks. The great threat of the SIM-swap attack is that it is social in nature and thus not technically complex. As such, simply requiring a real password will eliminate the social nature of the hack.[70] Thus, a low-cost measure of requiring real passwords to transfer a wireless customer's phone number, which effectively functions as the key to her digital life, will greatly limit the danger of SIM-swap attacks. Such a low-cost solution to avoid the millions of dollars in injuries harming wireless customers strongly indicates that wireless providers are the least cost avoider. With this low-cost solution in reach, economic theory—and intuition—place liability for SIM-swap attacks on wireless providers.

---

[68] CALABRESI, *supra* note 49, at 143–44.

[69] *Id.* at 150–52. Indeed, wireless providers likely have monopoly or near monopoly power such that the cost of avoidance measures for SIM-swap attacks can quickly be distributed to wireless customers with minimal transaction costs, whereas direct assignment to wireless customers would accomplish little harm reduction.

[70] Although additional issues may arise with forgotten passwords and weak passwords, as discussed in Section II, requiring any password is still an improvement. More recent evidence has shown that wireless provider employee bribery is also a vulnerability. Lecher, *supra* note 17. Ultimately, the exact solution is to require wireless providers to implement reasonable standards of security according to a reasonable standard of care, as argued below in Section IV. Such a determination will require some examination of the facts, but it will also lend itself to a reasonable and intelligent standard that can shift over time with changes in cybersecurity threats and technology. A reasonableness standard will also force wireless providers to secure their own systems and employees, which the wireless customer has no ability to control.

C. Wireless providers should be liable for SIM-swap attacks because wireless providers are the most competent avoider

Not only are wireless providers the least cost avoiders, they are also the most competent avoider. As gatekeepers, administrators, builders, and providers of wireless networks, wireless providers are best situated to understand the vulnerabilities of their own network, especially with rapid technological change, and to control the actions of their employees. In contrast, other relevant parties are unlikely to provide adequately competent and responsive solutions.

Technology is rapidly changing, leading to new opportunities and benefits on the one hand but also to new risks and dangers on the other. Because of the rapidly changing and increasingly complex nature of technology, few people are adequately knowledgeable and competent to address the risks. The average consumer is likely neither able nor competent enough to prevent SIM-swap attacks because there is little the consumer can do and there are few consumers who understand, or are even aware of, the vulnerabilities.[71] Just as product liability places liability on manufacturers for defects because products are too complex for consumers to adequately understand the threat of defects, cybersecurity negligence must place the liability on wireless providers for SIM-swaps because cybersecurity has become too complex for consumers to adequately understand the threat of vulnerabilities.[72]

Further, legislatures still lack the competence to adequately address rapidly developing vulnerabilities. Legislatures may pass legislation that places liability directly on the wireless providers as the most competent avoiders. Going further than that to create complex reactionary legislation that addresses each problem as it comes will recreate the current problem. Right now, there is specific legislation governing cybersecurity standards for certain industries, e.g., banking and healthcare, but these are not the only places where cybersecurity is an issue.[73] Rather, SIM-swap attacks on

---

[71] This parallels the inadequate knowledge externalization of the second guideline in the least cost avoider analysis in Section III.B. CALABRESI, *supra* note 49, at 148–49. Thus, placing the burden on consumers would run afoul of the second guideline because consumers generally lack adequate knowledge to prevent the harm. This section focuses on competence for an intuitive argument while Section III.B focuses on externalities for an economic argument, but both arguments center on the simple proposition that consumers are just not competent enough to bear the burden of ensuring cybersecurity.

[72] Jeffrey W. Kemp & Lindsy Nicole Alleman, *The Bulk Supplier, Sophisticated User, and Learned Intermediary Doctrines Since the Adoption of the Restatement (Third) of Torts*, 26 REV. LITIG. 927, 928 (2007).

[73] Indeed, targeted regulation and liability for cybersecurity practices have been discussed in detail in other contexts. *See, e.g.*, David L. Silverman, *Developments in Data Security Breach Liability*, 70 BUS. LAW. 231 (2015); Simpson, *supra* note 31; Feigelson & Calman, *supra* note 62; Hahn & Layne-Farrar, *supra* note 47; Ritu Singh, *Two-Factor Authentication: A Solution to Times Past or Present? The Debate*

wireless providers pose even greater threats in some cases. Comprehensive legislation from a legislature marginally more competent than consumers to address rapidly developing cybersecurity threats in the wireless and internet industries will only continue the cycle of delayed responses following significant harms.[74] The legislature is neither responsive nor competent enough to properly respond to these threats.

Finally, though much more technically competent, administrative agencies such as the Federal Communication Commission (FCC) and the Federal Trade Commission (FTC) still have insufficient responsive competence to adequately address rapidly developing vulnerabilities. The FTC and the FCC can bring about industry-wide progress towards improved standards for consumer privacy and data security, but these agencies also respond slowly to significant consumer injury.[75] Both the FTC and the FCC lack the responsive competence to rapidly adjust to developments in cybersecurity threatening the wireless and internet industries. Thus, the FTC and the FCC can help bring about progress, but that does not justify shielding the most competent avoiders, wireless providers, from liability for SIM-swap attacks.

Thus, wireless providers are the most competent party to understand the vulnerabilities of their own network and avoid SIM-swap attacks, and the other relevant parties are insufficiently competent or unresponsive.

Surrounding the Gramm-Leach-Bliley Security Safeguards Rule and the Methods of Risk Assessment and Compliance, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 761 (2006). Examples of targeted legislation include the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act, the Controlling the Assault of Non-Solicited Pornography and Marketing Act, the Electronic Communications Privacy Act (ECPA), the Children's Online Privacy Protection Act, and the Graham-Leach-Bliley Act. *See, e.g.*, 45 C.F.R. Part 164 (2018); 15 U.S.C. § 1681 et seq. (2012); 15 U.S.C. §§ 7701–7713 (2012); 15 U.S.C. §§ 6801–6809 (2012). The ECPA may be relevant to SIM-swap attack victims in that it may impart statutory liability on wireless providers, but that additional analysis is beyond the scope of this note.

[74] For an argument that "legislation has fallen short in mitigating the threat of cyber-attacks," *see* Christine Lino, *Cybersecurity in the Federal Government: Failing to Maintain a Secure Cyber Infrastructure*, 41 BULL. ASS'N FOR INFO. SCI. & TECH. 24, 25–26 (2014) (noting specifically the Senate's failure to pass the Cybersecurity Act of 2012).

[75] *See* discussion *infra* Section IV.A. The FTC has recognized the threat of SIM-swap attacks and the FCC has addressed the threat of "pretexting" (i.e., fraudulent impersonation of an account owner to achieve unauthorized account access), but both agencies have failed to place distinct liability on the wireless providers or provide recourse for harmed victims. *See, e.g.*, 47 C.F.R. § 64.2010 (2018).

IV. LAW-BASED ARGUMENTS: WIRELESS PROVIDERS ARE LIABLE FOR UNAUTHORIZED ACCOUNT ACCESS AND SIM-SWAP ATTACKS UNDER EXISTING FEDERAL REGULATION AND TORT COMMON LAW, BUT TORT COMMON LAW PROVIDES THE MOST ELEGANT SOLUTION

A. Federal law, administrated by both the FCC and the FTC, assigns liability to wireless providers, but uncertainty and delayed enforcement harms consumers

Liability for SIM-swap attacks should attach to wireless providers under existing federal law, but the liability is accompanied with uncertainty and delayed enforcement to the point that SIM-swap victims may be left out in the cold. The FCC and the FTC both exert influence over wireless providers in the context of data privacy and security. The FCC regulates everything under the telecommunications umbrella, which includes wireless providers.[76] The FTC has taken the lead to enforce minimum standards of data privacy and security for consumer protection.[77] Thus, wireless providers should be answerable to both the FCC and the FTC for SIM-swap attacks, but reality is far more uncertain.[78] Wireless providers likely will continue to fly between the large cracks created by FCC and FTC policy.

1. In its role regulating wireless providers and phone numbers, the FCC should ensure proper assignment of liability for SIM-swap attacks, but such liability is uncertain in reality

Under its governing laws, the FCC should assign and enforce wireless provider liability for SIM-swap attacks. However, the FCC's actions and position remain uncertain. Two primary factors support the claim that the FCC should ensure proper liability assignment for unauthorized number ports, i.e., SIM-swap attacks. First, the FCC's rules on wireless local number portability (WLNP), established under the authority of the Telecommunications Act of 1996, require the mechanism that enables SIM-swap attacks: number porting.[79] However, the regulations governing WLNP are silent about authorization.[80] Second, the Telecommunications Act of

---

[76] 47 U.S.C. § 151 (2012) ("For the purpose of regulating interstate and foreign commerce in communication by wire and radio . . . there is created a commission to be known as the 'Federal Communications Commission,'. . . .").

[77] 15 U.S.C. § 45 (2012).

[78] *See, e.g.*, Silverman, *supra* note 73; Simpson, *supra* note 31; Feigelson & Calman, *supra* note 62; Hahn & Layne-Farrar, *supra* note 47.

[79] 47 U.S.C. § 251(b)(2) (2012); 47 C.F.R. § 52.31 (2018); *see also* FED. COMMUNICATIONS COMM'N, *Wireless Local Number Portability*, May 18, 2016, https://www.fcc.gov/general/wireless-local-number-portability-wlnp [https://perma.cc/K7S9-932B].

[80] 47 C.F.R. § 52.31 (2018).

1996 requires telecommunications providers, including wireless providers, to protect proprietary customer information.[81] Thus, the FCC has both mandated the process giving rise to SIM-swap attacks, while ignoring the risk created, and has responsibility for ensuring protection of customer information. Unfortunately, the FCC's clear responsibility and role for resolving SIM-swap attacks is muddied by uncertainty arising from the FCC's slow responsiveness and inconsistent focus.

The Telecommunications Act provided several protections to wireless customers that should provide protection for SIM-swap attacks. Specifically, if a wireless provider fails to protect the confidentiality of customer proprietary information, the FCC can levy charges and penalties.[82] Even more relevant to the SIM-swap victim, the customer can sue for the full amount of damages—including reasonable attorney's fees—sustained by a customer information violation.[83] Such a private right of action against wireless providers certainly would and should provide wireless customers harmed by SIM-swap attacks with proper protection and recourse for unauthorized account access.[84] Unauthorized control of a customer's account and phone number surely must be an unauthorized disclosure of customer proprietary information under the statute.[85] The statute defines Customer Proprietary Network Information (CPNI) as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service . . . " and "information contained in the bills. . . ."[86] Although the statute targets account usage information, excluding coverage over control and access of an entire account while protecting things like "information contained in the bills" is the equivalent

[81] Telecommunications Act of 1996, Pub. L. No. 104–104, 110 Stat. 56 (1996) (codified as 47 U.S.C. § 222 (2012)); 47 U.S.C. § 332 (2012). Other laws make unauthorized account access illegal, but do not address wireless provider duties. Wireless Telephone Protection Act of 1998, Pub. L. No. 105–172, 112 Stat. 53 (1998) (primarily amending 18 U.S.C. § 1029). *See also* FED. COMMUNICATIONS COMM'N, *Cell Phone Fraud*, Sept. 8, 2017, https://www.fcc.gov/consumers/guides/cell-phone-fraud [https://perma.cc/EHY5-U9BK].

[82] 47 U.S.C. § 205 (2012).

[83] *Id.* §§ 206–07.

[84] The scope of these privacy protections afforded by the FCC under 47 U.S.C. § 222 was expanded by FCC regulations to cover internet service providers (ISPs), but those regulations were repealed recently. Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 Fed. Reg. 87274 (Dec. 2, 2016) (to be codified at 47 C.F.R. pt. 64), *repealed by* Act of Apr. 3, 2017, Pub. L. No. 115-22, 131 Stat. 88 (codifying a joint resolution disapproving of the FCC's broadband customer privacy rules). *See* Paul R. Gaus, *Only the Good Regulations Die Young: Recognizing the Consumer Benefits of the FCC's Now-Defunct Privacy Regulations*, 18 MINN. J.L. SCI. & TECH. 713 (2017).

[85] 47 U.S.C. § 222 (2012).

[86] *Id.* § 222(h)(1). Note that CPNI excludes "subscriber list information," which includes telephone numbers. Yet, the telephone number itself is not the problem in a SIM-swap attack; unauthorized control of the entire account and the telephone is the problem.

of locking the window while leaving the door wide open.[87] Even reading the statute in the most literal sense, handing over complete control of the account certainly exposes even the most narrowly defined CPNI to the unauthorized hacker. Thus, the Telecommunications Act directly provides for wireless provider liability in the case of SIM-swap attacks.

Unfortunately, wireless provider liability only becomes more uncertain by looking to FCC guidance and case law. The privacy protections required by 47 U.S.C. § 222 focus on information disclosure as opposed to reasonable security measures.[88] As such, there is no guidance on what security measures are necessary to fulfill the "duty to protect the confidentiality of proprietary information of . . . customers."[89] Further, the FCC has not issued any guidance on reasonable data security nor undertaken any enforcement actions, and the case law surrounding the issue is only tangentially relevant.

Although the FCC may ultimately address the issues, the case law illustrates the FCC's inability to respond quickly to address customer harms. The initial implementation of WLNP took years to resolve in the courts, but the FCC eventually won.[90] Further drawn-out battles were fought over how customer information could be used during wireless number ports, but the FCC eventually won.[91] Still more drawn-out battles were fought over the type of customer approval required for wireless providers to disclose customer proprietary information, but the FCC eventually won.[92]

The most relevant case law addresses the private right of action under 47 U.S.C. § 206 for violations of 47 U.S.C. § 222, but such actions are sparse. *Weinstein v. AT&T Mobility LLC* examines the extent an undirected employee's actions in violation of 47 U.S.C. § 222 subject the wireless provider to liability.[93] In *Weinstein*, the plaintiff sued AT&T under 47 U.S.C. §§ 206 and 222 because an AT&T employee used her position to access information about the plaintiff and send messages regarding the plaintiff's relationships to the plaintiff's contacts.[94] The court held that employees

---

[87] *Id.* § 222(h)(1)(B).

[88] *Id.* § 222.

[89] *Id.* § 222(a).

[90] *See, e.g.*, Cellular Telecommunications & Internet Ass'n v. F.C.C., 330 F.3d 502, 504 (D.C. Cir. 2003) (ending delays to the rollout of WLNP).

[91] *See, e.g.*, Verizon California, Inc. v. F.C.C., 555 F.3d 270, 272–75 (D.C. Cir. 2009) (upholding the FCC's order based on customer privacy in 47 U.S.C. § 222 and prohibiting Verizon from using customer proprietary information received from a competitor for marketing purposes before completing the number transfer to the competitor's network).

[92] *See, e.g.*, National Cable & Telecommunications Ass'n v. F.C.C., 555 F.3d 996, 997, 999–1002 (D.C. Cir. 2009) (upholding the FCC's order based on 47 U.S.C. § 222 requiring wireless providers to obtain opt-in consent before disclosing customer proprietary information).

[93] 553 F. Supp. 2d 637, 639–41 (W.D. Va. 2008).

[94] *Id.* at 638–39.

acting outside their scope of employment do not subject the wireless provider to liability under 47 U.S.C. § 222.[95] The court also held that the wireless provider was not liable because no recoverable damages were specified in the absence of any "injury to [the plaintiff's] person, property, health, or reputation."[96]

Thus, *Weinstein* is an example of an unsuccessful suit under 47 U.S.C. §§ 206 and 222, but SIM-swap attacks are easily distinguishable. First, unlike the employee in *Weinstein*, wireless provider employees who transfer phone numbers are acting within the scope of employment.[97] Second, unlike in *Weinstein*, cryptocurrency theft in a SIM-swap attack provides concrete and cognizable injury to a customer's property.[98]

When viewing the statute and case law holistically, the Telecommunications Act does provide SIM-swap victims a path to obtain recourse from wireless providers, but there is little clarity on the standards courts will apply to wireless providers. Suits under 47 U.S.C. §§ 206 and 222 do not appear to have been successfully brought, but SIM-swap attacks are easily distinguished from the failed suits. The FCC has not published an order setting a standard for privacy, and generally is slow to do so and even slower to enforce it—especially considering the drawn-out court battles that inevitably follow.[99] If the FCC does take up the issue, SIM-swap victims are likely to be better protected in the long term, but the FCC's history indicates that SIM-swap victims who have already been harmed, or are currently being harmed, will receive little recompense. These multiple factors combine to form the conclusion that the Telecommunications Act does assign liability for SIM-swap attacks to wireless providers, but significant uncertainty caused by the slow responsiveness of the FCC provides little assurance that a suit against a wireless provider will be successful.

---

[95] *Id.* at 640–41.

[96] *Id.* at 640.

[97] *Id.* However, in cases where customer account passwords are disclosed or bypassed by bribed wireless provider employees, the argument for wireless provider liability under 47 U.S.C. § 222 may be weakened by the holding in *Weinstein*. That is, *Weinstein* might be interpreted to hold that wireless providers are not liable under 47 U.S.C. § 222 for SIM-swap attacks enabled by unscrupulous, undirected employees.

[98] *Id.* at 640–41.

[99] The closest thing appears to be regulation in 47 C.F.R. § 64.2010 prohibiting unauthorized access to customer proprietary network information and requiring adequate customer authentication steps.

2. In its role as the default data security and privacy regulator, the FTC should enforce prevention of SIM-swap attacks, but SIM-swap victims will receive little recourse

The FTC has become the leading agency in regulating data security and privacy, and thus should enforce measures to prevent SIM-swap attacks.[100] However, two significant issues exist that limit the wisdom of relying on the FTC to solve SIM-swap attacks. First, FTC action against wireless providers may be limited because wireless providers provide common carrier services.[101] Second, FTC action against wireless providers may cause change to wireless industry standards for security, but it would not provide any direct mechanism for SIM-swap victims to recover damages.

The rise in the FTC's authority over data privacy and security is due to the absence of another agency in this role and a broad reading of the FTC's power to prevent "deceptive" or "unfair" activities under section 5 of the Federal Trade Commission Act (FTCA).[102] The FTC has taken the initiative to bring two kinds of enforcement actions against companies with poor data security and privacy procedures: actions based on the first prong of deceptiveness and actions based on the second prong of unfairness.[103]

Under the deceptiveness prong, the FTC has brought actions against entities for failing to abide by their own data privacy and security policies.[104] In such cases, the FTC asserted that luring in consumers with promises of privacy and security is deceptive when the entity fails to act as promised.[105] These actions have generally been successful.[106] However, the deceptiveness prong requires that the misbehaving entity make promises and then fail to deliver.[107] Thus, the deceptiveness prong is inapplicable for entities promising no or only dismal data privacy and security.[108]

Due to the limitations of the deceptiveness prong, the FTC has subsequently brought actions under the unfairness prong against entities with either no data privacy and security policy or a poor one.[109] These actions

---

[100] Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 239–44 (2017).

[101] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 598–99 (2014).

[102] Federal Trade Commission Act, 15 U.S.C. § 45(a) (2012).

[103] Pardau & Edwards, *supra* note 100, at 233–35; Simpson, *supra* note 31, at 692–96. Note that this area of law is undergoing significant development.

[104] *Id.* at 237–41.

[105] *Id.* at 237–38, 251–52.

[106] *Id.* at 239–42.

[107] *Id.* at 237.

[108] *Id.* at 238.

[109] *Id.* at 241–43; Solove & Hartzog, *supra* note 101, at 598–99.

assert that the entity was committing unfair acts by subjecting consumers to nonexistent or dubious data privacy and security procedures that exploit consumers in a way competitors are unwilling to match.[110] In other words, exploitation of consumers provides an unfair advantage over competitors who have a conscience.

The FTC has brought a large number of actions under the deceptiveness prong against entities that do not follow their own data protection policies.[111] Furthermore, courts have endorsed the FTC's authority to bring this kind of action.[112] However, actions under the unfairness prong have less precedential support because fewer have been brought and most have settled.[113] Nonetheless, the FTC's authority to bring actions under the unfairness prong for inadequate data privacy and security procedures has been specifically endorsed by the Third Circuit in *F.T.C. v. Wyndham Worldwide Corp.* and has not been rejected by any court.[114] Though often calling for comprehensive legislation on data privacy and security, the FTC has, in the absence of such legislation, taken up the mantle of data privacy and security enforcer by pursuing entities with no standards, insufficient standards, or standards they fail to meet.[115] Thus, the FTC is by default the closest thing to a general data privacy and security regulator. As such, one would expect that the FTC should have a role in pursuing improved wireless account security measures to prevent SIM-swap attacks.

However, the FTC may have limited ability to regulate wireless providers.[116] Specifically, the Ninth Circuit recently held in its *en banc* decision, regarding wireless provider AT&T, that the FTC can only bring actions against common carriers under section 5 of the FTC Act for their

---

[110] Pardau & Edwards, *supra* note 100, at 229.

[111] *Id.* at 239–41; Solove & Hartzog, *supra* note 101, at 598–99.

[112] Pardau & Edwards, *supra* note 100, at 239–41.

[113] *Id.* at 239–43.

[114] 799 F.3d 236, 247–49 (3d Cir. 2015) (finding that the FTC had authority to bring suit under the unfairness prong of Section 5). *But see* LabMD, Inc. v. F.T.C., 678 F. App'x 816, 817, 819–21 (11th Cir. 2016) (granting a stay for appeal to the Eleventh Circuit because LabMD made "a strong showing" that the FTC's interpretation of the injury requirement under section 5 of the FTCA is unreasonable). However, the Eleventh Circuit on appeal assumed that the FTC's interpretation of the unfairness was proper but found that the resulting cease and desist was too ambiguous to be enforceable. LabMD, Inc. v. F.T.C., 894 F.3d 1221, 1231, 1236–37 (11th Cir. 2018). A holding in LabMD's favor on interpretation of the unfairness prong would have limited the FTC's effective regulatory power to enforcement actions having more than a significant risk of causing tangible harms. *See* Pardau & Edwards, *supra* note 100, at 262–63.

[115] Pardau & Edwards, *supra* note 100, at 239–42.

[116] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1428–29 (2017); Simpson, *supra* note 31, at 692–96.

non-common carrier activities.[117] This matter is not fully settled as the designation of wireless providers as common carriers for certain services is still fluid.[118] In view of these developments, the FTC's authority to bring enforcement actions against wireless providers for insufficient security leading to SIM-swap attacks remains uncertain. Wireless account access, with its close relation to the provision of mobile voice, a common carrier service, very possibly still qualifies for the common carrier exception to the FTC's authority even under the Ninth Circuit's holding that the exception is activity-based and not status-based.[119] Thus, although the FTC has a substantial role in general data security and privacy, there is strong doubt as to the FTC's regulatory authority to enforce data privacy and security standards against wireless providers' provision of common carrier services.

But, even assuming the FTC does have authority to bring actions against wireless providers for SIM-swap attacks, such actions would not provide any direct benefit to SIM-swap victims. In other words, the FTC's authority to sue wireless providers does little to provide recovery of damages for SIM-swap victims. Thus, the so-called default cybersecurity agency is in a position where it may have no ability to bring actions based on SIM-swap attacks and, even if it does have authority such actions will do little to make SIM-swap victims whole. Certainly, the FTC should get involved to solve the problem of SIM-swap attacks, but any comprehensive solution that addresses the injuries suffered by SIM-swap victims must go beyond FTC action.

B. Tort common law assigns liability to wireless providers for negligence, which protects consumers now and provides relief for SIM-swap victims

Wireless providers should be subject to liability for SIM-swap attacks according to a negligence standard. As both the least cost avoider and the most competent harm avoider, wireless providers are in a unique position to address the risks of SIM-swap attacks. Tort law and the negligence standard are properly situated to place the liability on wireless providers. Although other routes to address SIM-swap attacks exist, including FCC or FTC action and rulemaking, these mechanisms are slow to respond to consumer harms and provide uncertain recourse for SIM-swap victims. In contrast, civil negligence liability is available now and provides clear recourse for SIM-

[117] Fed. Trade Comm'n v. AT&T Mobility LLC, 883 F.3d 848, 863–64 (9th Cir. 2018) (*en banc*); *see also* Simpson, *supra* note 31, at 692–96.

[118] *See AT&T Mobility*, 883 F.3d at 864.

[119] *Id.* at 863.

swap victims.[120] Further, a reasonable standard of care for cybersecurity provides a fluid standard that can change with the development of new threats and new technology standards. Courts should find wireless providers liable for injuries arising from SIM-swap attacks under the reasonable standard of care. This section leans on case law from the U.S. Courts of Appeals for support and substantially distinguishes contrary holdings before developing the argument that negligence with a reasonableness standard is the most elegant solution for SIM-swap attacks.

Although case law regarding wireless provider liability for SIM-swap attacks is lacking, inferences can be drawn from negligence claims brought for alleged insufficient data security. These inferences strongly support a negligence claim against wireless providers for SIM-swap attacks based on the presence of tangible, nonspeculative harm, which starkly distinguishes SIM-swap attacks from cases where courts have held against finding liability for negligence due to the absence of such harm.

Specifically, SIM-swap attacks involving theft of cryptocurrency assets are distinguishable from many failed negligence claims because such SIM-swap attacks include tangible assets that establish clear harm. For example, due to the absence of harm, the court in *Ruiz v. Gap, Inc.* upheld summary judgement, rejecting a negligence claim arising from theft of personal information on a computer.[121] According to the court, theft of this personal information "failed to establish sufficient appreciable, nonspeculative, present harm."[122] Thus, unlike the absence of nonspeculative, present harm in *Ruiz*, SIM-swap victims can identify cryptocurrency assets with substantial and easily determinable value.[123]

Indeed, courts often focus on the presence or absence of tangible damages in negligence claims, an issue strongly supporting recovery for SIM-swap victims who have suffered theft of millions of dollars. Specifically, the court in *Anderson v. Hannaford Bros. Co.* held that mitigation costs incurred responding to increased threat of fraud qualified as reasonably foreseeable and cognizable injury.[124] In that case, the negligence claim flowed from the theft of defendant grocery store's electronic customer

---

[120] Two lawsuits filed against wireless providers by SIM-swap victims allege negligence, among other things. *Terpin Complaint*, *supra* note 24, ¶¶ 183-91; *Tapang Complaint*, *supra* note 24, ¶¶ 7.1-7.4.

[121] 380 F. App'x 689, 691 (9th Cir. 2010).

[122] *Id.*

[123] *Id.* Some negligence claims have been barred against financial institutions due to specific regulations. *See, e.g.*, Patco Const. Co. v. People's United Bank, 684 F.3d 197, 199, 216 (1st Cir. 2012) (affirming dismissal of the negligence claim for fraudulent fund transfer because the bank's duty of care was displaced by Article 4A of the UCC, which governs funds transfers).

[124] 659 F.3d 151, 154, 164–65, 167 (1st Cir. 2011).

payment information.[125] The court reversed dismissal of the negligence claim.[126] Cryptocurrency assets stolen from SIM-swap victims, which have an easily determinable U.S. dollar value, are even more cognizable than the mitigation costs supporting the negligence claim in *Anderson*.[127]

As another example of a negligence claim supported by financial injury, the court in *Resnick v. AvMed, Inc.* held that a negligence claim was supported by monetary losses due to fraudulent charges.[128] The court reversed dismissal of the negligence claim that flowed from defendant's alleged negligence in securing computer hardware that held personal customer information.[129] Just as the financial injury of monetary losses in *Resnick* supported a negligence claim for victims of personal information theft, the financial injury of lost cryptocurrency assets having real and clear monetary value supports a negligence claim for SIM-swap victims.[130]

Further, SIM-swap victims suffer from determinable damages that are not boundless, and these damages serve to identify a limited class of victims. In *Lone Star National Bank, N.A. v. Heartland Payment Systems, Inc.*, the court upheld the negligence claim based on the identifiability of the injured class and the absence of boundless liability due to the determinability of the damages.[131] The plaintiff met the requirement of "an identifiable class that the defendant should have reasonably foreseen was likely to be injured by the defendant's conduct," and the fraudulent charges and credit card replacement costs did not impart "boundless liability."[132] Thus, the court held the economic loss doctrine did not bar the negligence claim against the credit card processor for data breach.[133]

Thus, the clearly determinable and tangible damages along with the easily identifiable class of injured victims in SIM-swap attacks support negligence claims against wireless providers as illustrated by this brief survey of cases from U.S. Courts of Appeals. Even more, however, negligence provides a more elegant solution to SIM-swap attack than federal action. Negligence is the right solution because it is available to victims now, it is fluid enough to apply to the rapidly changing environment of cybersecurity threats, and it provides remedy to victims of SIM-swap attacks instead of promises of improvement in the future.

---

[125] *Id.* at 154.

[126] *Id.*

[127] *Id.* at 164–65, 167.

[128] 693 F.3d 1317, 1324, 1327–28 (11th Cir. 2012).

[129] *Id.*

[130] *Id.*

[131] 729 F.3d 421, 426 (5th Cir. 2013).

[132] *Id.* (citation omitted).

[133] *Id.*

First, although the FCC and the FTC may promote progress reducing SIM-swap attacks by successful rulemaking or enforcement actions, such steps are slow to implement and do little for the victims who have already lost millions of dollars. Negligence is a ready standard currently available to victims of SIM-swap attack, and it can accomplish the same goal of reducing SIM-swap attacks.[134] Second, negligence according to a reasonableness standard is also fluid enough to apply to the rapidly changing environment of cybersecurity threats. As threats develop, wireless providers should be held to a standard of reasonable security measures. Thus, as threats change and rapidly develop, the efforts that wireless providers take to ensure security can be judged for reasonableness against the changes and timing that occur in the industry.[135] Third, negligence also provides remedy to victims of SIM-swap attacks. Unlike FCC rulemaking, FTC action, or legislative reaction, negligence provides a way to make present victims whole. Such a fair treatment of the victims also furthers the public policy goal of consumer protection. By providing remedy to those harmed and placing the liability on wireless providers, negligence claims would change wireless provider behavior to avoid liability by exercising proper care during phone number transfers.

Assigning negligence liability under a reasonableness standard to wireless providers would help victims now, fluidly adapt to the changing threat landscape in the future, and provide remedy to victims while furthering consumer protection.

V. CONCLUSION AND RECOMMENDATION: TORT LAW IS AN ELEGANT SOLUTION FOR THE PRESENT; THE FTC AND FCC MIGHT HELP IN THE FUTURE

Wireless providers should be held to a reasonableness standard of negligence liability for SIM-swap attacks on wireless consumers. The current legal landscape provides uncertainty without a clear path forward for victims. Negligence liability provides that clear path today if courts will apply it. There are strong arguments for involvement by the FTC, as the default cybersecurity regulator, and the FCC, as the explicit telecommunications regulator, but such agency involvement will be too slow to prevent and remedy the harms occurring now and is accompanied by

[134] The FCC certainly should undertake rulemaking to clarify the requirements placed on wireless providers by 47 U.S.C. § 222, but such rulemaking should complement common law negligence claims by clarifying that the duty or care is set by a reasonableness standard and by explicitly assigning damages for SIM-swap attacks to wireless providers.

[135] A strict liability standard would not provide the same flexibility and may reduce consumer consumption of wireless services.

significant uncertainty. Tort law can provide the solution to SIM-swap attacks now by making wireless providers liable to SIM-swap victims for unreasonable security. Such liability will encourage the hoped-for improvements in wireless provider security. The FCC, FTC, and the federal legislature can and probably should help, but the problem might be solved before they get to it.