
What Is Your Mother's Maiden Name?

A Feminist History of Online Security Questions

ABSTRACT The history of online security questions demonstrates how hegemonic beliefs about gender and sexuality have come to dictate the terms of “authentic” selfhood in contemporary digital spaces. Best known for their role in web-based information management, security questions have a history in North America that stretches back more than a hundred and fifty years—from Irish immigrant banking in New York in the mid-nineteenth century, to the rise of personal computing in the 1970s and 1980s, to today. Across this history, security questions have been structured around heteronormative expectations about users’ lives and relationships. This is nowhere more evident than in the canonical security question, “What is your mother’s maiden name?” To trace the evolution of the security question, this article surveys industry writings on authentication protocols from the 1850s to the present. It argues for a reevaluation of the often-unquestioned logics that perpetuate discrimination through technologies of data. **KEYWORDS** authentication protocol, gender discrimination, heteronormativity, pre-digital data, security questions

The story of the online security question is a story of data and its discontents—one that can be traced to a moment of profound cultural shift that far predates the digital. This history speaks to the ways that concepts of personal information have come to dictate the terms of contemporary identity through hegemonic notions of gender and sexuality. Although security questions are best known today for their role in web-based information management, their history stretches back more than a hundred and fifty years. Originally implemented in New York in 1850 by Emigrant Industrial Savings Bank, an institution created to serve Irish immigrants who faced ethnic discrimination at other banks, the security question had been adopted widely in the US banking sector by the turn of the twentieth century. In the 1970s and 1980s, the earliest days of personal computing and consumer Internet access, the first computer security experts borrowed heavily from banks in setting standards for database authentication. These standards have continued to shape the protocols through which the

Feminist Media Histories, Vol. 3, Number 3, pps. 57–81. electronic ISSN 2373-7492. © 2017 by the Regents of the University of California. All rights reserved. Please direct all requests for permission to photocopy or reproduce article content through the University of California Press’s Reprints and Permissions web page, <http://www.ucpress.edu/journals.php?p=reprints>. DOI: <https://doi.org/10.1525/fmh.2017.3.3.57>.

information that is imagined to establish authentic personhood is collected, processed, and used to determine access on the Internet, bringing the mid-nineteenth-century technology of the security question, and the discriminatory beliefs that helped shape it, well into the twenty-first.

Like the concept of data itself, the security question has evolved over the course of its history.¹ It has gone by many names, including “test question,” “challenge question,” “question-and-answer password,” and (most poetically) “shared secret.”² The premise of these questions, however, remains the same. An account holder must prove their identity by correctly responding to a question that, it is presumed, only they can answer. While they are still widely used in digital spaces, researchers have recently begun arguing against security questions in favor of more reliable forms of identity verification.³ Yet, even as the online security question is entering its decline, its legacy remains foundational to the structural logics that define “true” personhood in digital spaces. Along with the security question has come an underlying set of problematic, heteronormative assumptions about what kinds of data should be used to establish and verify identity. With notable frequency, both at present and across their history, security questions have required users to produce answers that comply with heteronormativity—that is, dominant heterosexual and cisgender norms for experiences of and attitudes toward femininity, masculinity, romance, reproductivity, and family relationships. This is nowhere more evident than in the most canonical of security questions, “What is your mother’s maiden name?”

Delineating the history and cultural implications of the security question through a feminist lens offers us the opportunity to deconstruct, critique, and reevaluate unjust yet widely accepted standards of knowledge making that fail to account for realities of queer subjects and others who do not conform to heteronormative expectations. In this way, the history of the security question resonates with larger questions around the role of data in our contemporary society. As others have argued, the very notion of objective data, especially when it is used to dictate the terms of identity, can enact oppression against those whose lives do not fit with the basic presuppositions that underlie how that data has been conceptualized.⁴ Tracing the evolution of the security question also sheds light on a larger cultural shift in how a person’s authentic selfhood is understood through their personal information—a shift that began in the mid-nineteenth century. Although the concept of data predates the emergence of the security question, the rise of the security question points toward a meaningful change in how societal institutions, for instance banks, have conceived of what makes personal information reliable, meaningful, and of value.⁵ Specifically, as

we will see, security questions represent a move away from embodied and/or interpersonal modes of knowing toward standardized, discrete, and theoretically immutable units of information. The adoption of the question-and-answer system can be seen as a formative step in a new social imagining of “real” identity as a collection of discrete data points. Because the function of security questions is to facilitate and restrict access, these seemingly simple protocols encapsulate larger societal dynamics of power. For this reason, any meaningful telling of the history of online security questions must be by nature a feminist history. Such a history prompts a wide-reaching reevaluation of the cultural beliefs that dictate the terms of legitimate subjecthood, both in the present moment and in the proto-digital past.

METHODS, INTERLOCUTORS, AND INTERVENTIONS

In order to tell the history of the online security question, in both its digital and pre-digital contexts, this work surveys and critiques industry writing on authentication protocols from the 1850s to the present. Beginning with the digital age and moving backward into the security question’s nineteenth-century origins, I also draw from an extensive list of commonly used contemporary online security questions and read this list against paperwork documenting early bank account management protocols. Although the security question and its effects on contemporary standards of identity verification have now been implemented across the globe, my focus here is on the American context from which the security question emerged, and where a number of key companies that are core to what we might call today’s online identity landscape have their primary operations. Together, these materials allow me to trace how the “mother’s maiden name” question and others like it—beginning from their roots in early US immigrant banking, on through the widespread adoption of personal computing devices in the 1990s, and up to the present day—have both illustrated and deeply influenced shifts in technologies of identity verification and conceptualizations of the relationship between gender, sexuality, and selfhood.

In its conceptual framework, my work draws from foundational scholarship in the area of feminist technology studies, such as that by Wendy Chun and N. Katherine Hayles, and in particular writing by Lisa Nakamura on how identity is coded in digital spaces through both cultural and technological processes.⁶ Existing published research on online security questions and digital authentication practices more generally (such as that cited and critiqued below) has focused almost exclusively on the neoliberal concern of effectiveness: whether or not security questions succeed at keeping accounts secure. The present work,

by contrast, is not interested in optimizing authentication techniques, but in laying bare the social forces and often unspoken biases that continue to affect measures of selfhood with which digital subjects must engage as a basic precondition for operating online. It is my belief that a greater awareness of this history can help guide us toward more conscientious, inclusive protocols that account for and respect those subjects whose lives do not fit with dominant, culturally determined markers of authentic identity.

This work also builds on existing historical research on technologies of identity documentation as they emerged, shifted, and became codified in the United States across the nineteenth and twentieth centuries. Most notably, Craig Robertson's history of the American passport similarly addresses how contemporary identification technologies (for instance the technology of the passport itself) are inextricably tied to the experiences of immigrants to America, as well as broader, often discriminatory cultural perceptions of immigration. Robertson's work likewise seeks to explain how a specific approach to documenting selfhood "came to be accepted as a reliable answer to the question, 'Who are you?'"⁷ Robertson has described the identification processes of modern society as "a documentary regime of verification," founded on a belief that an individual's true, official identity can be classified and catalogued through the collection of specific, objective facts.⁸ Across its many incarnations, the security question can itself be understood as a tool within larger regimes of verifications. At the same time, however, a feminist history of the security question supplements and perhaps even complicates research by scholars like Robertson in two key ways. First, this work brings the mid-nineteenth-century history of identity authentication explicitly into dialogue with digital protocols of the twenty-first century. Second, it underscores the importance of gender and sexuality to documentary regimes of verification and the notions of selfhood that they both reflect and engender.

In recent years, the discrimination enacted through digital authentication practices, especially as such practices relate to the constructs of heteronormativity, has been most visible in debates around the affordances and policing of Facebook profiles. As Rena Bivens explains in her 2015 essay "The Gender Binary Will Not Be Deprogrammed: Ten Years of Coding Gender on Facebook," the options that Facebook offers (or does not offer) when it requires users to declare their gender identities have deep effects as well as social implications—effects both on users who may feel themselves unwelcome on the site if their gender is not meaningfully represented, and on Facebook's advertising marketing strategies, which rely heavily on codifications of gender. In this way,

the design of profiles on sites like Facebook represents “powerful . . . productive force[s] in the broader software-user relationship . . . [which] can produce the conditions for gendered existence.”⁹ The stakes for these “conditions for gendered existence” become clearer when we consider the rhetoric of authenticity. Bivens describes how Facebook has increasingly espoused a narrative of “realness,” invoking moralistic language to discourage users from creating fake accounts, and suggesting in no uncertain terms that trustworthy individuals only give real personal information when they register for accounts. However, realness is itself a social construct. When companies such as Facebook ignore this fact, they inevitably enact discrimination. Facebook’s “real name” policy, for instance, has led to the marginalization and even erasure of queer and Native American users, whose accounts were deleted because their names did not conform to dominant standards for what appears “normal.”¹⁰ This point is crucial to understanding why critiquing the gender and sexual expectations that underlie security questions matters. The very structures through which identity is recorded and verified are designed around presumptions that often make it impossible for subjects who are nonnormative—whether in their gender, their name, or their personal history—to represent themselves authentically, even as the digital systems that structure their daily lives demand that they perform this (impossible) authenticity.

Key to this work are notions of heteronormativity, homonormativity, and how non-straight, non-cisgender subjects may build their own lives and their interpersonal connections in ways that do not conform to contemporary standards of data. For this reason, I am also drawing from work by queer theorists such as Jack Halberstam and Elizabeth Freeman, especially their writing around “chrononormativity”—the expectation that “normal,” straight, cisgender lives follow a set path through love, marriage, children, et cetera—and alternative forms of relationality through queer kinship.¹¹ Even outside the realm of queer theory, there is precedent in the study of scientific knowledge making for thinking about how conceptualizations of supposedly objective data are in fact intimately tied to dominant notions of community building and family formation.¹² This essay extends that existing work, explicitly looking to the presence of gender and sexuality, with attendant issues of family and romance relationships, over the history of the security question.

ONLINE SECURITY QUESTIONS: A DIGITAL HISTORY

In a computational context, security questions have been used to verify identity for more than thirty years. To call these “online” questions perhaps suggests that

they are relatively new additions to the field of computer-mediated data management. In fact, their connection to computing can be traced across a much longer timeline. Security questions appear in discussions of data security even before the rise of the World Wide Web, when the Internet as many know it today began to take form. Much of the rhetoric used in these discussions serves as a window onto the moralistic belief systems that have structured concepts of authentication since the first days of digital information management. As early as 1987, when desktop terminals were becoming increasingly common in the workplace, information systems researchers identified what was already being seen as the prime risk inherent in connecting users to remote databases: unauthorized access. In “Verifying the Authentication of an Information System User,” a report from which many other experts in database management drew throughout the early 1990s, Niv Ahituv, Yeheskel Lapid, and Seev Neumann called this the “severe problem of authenticity,” a key component of which is a worry they articulate thus: “Is the user who is calling [the database] the one who is authorized to issue the call or a *pretender*?”¹³ To address this problem, the authors recommend that database administrators authenticate users through a combination of passwords and questions about personal and family history.¹⁴ I emphasize the word “pretender” here to draw attention to the language of authentic versus “pretend” identity that circulates around security questions—which quite literally do the work of “authentication.”

The history of the online security question is also a history built on repeating and reinforcing uninterrogated assumptions about identity. This can be seen in the way that today’s most common online security questions came into use. By 1991, the implementation of security questions for database management had emerged as a subject of specific research interest; it was through this research that the modern security question as it would later come to appear took shape. Work from this time standardized the expectation among experts that database administrators should incorporate security questions in addition to passwords, providing a second layer of defense against intrusion. William J. Haga and Moshe Zviran, in another influential study, “Question-and-Answer Passwords: An Empirical Evaluation” (1991), encouraged the implementation of “non-trivial” questions—that is, questions whose answers will be memorable for the user but cannot easily be found out or guessed. Some examples from the list of security questions that Haga and Zviran considered effective included “What is the name of your favorite uncle?” and “What was the name of your first boy friend/girl friend?”¹⁵ The implications of deeming this particular information exceptionally “non-trivial” are many, and to this day, many of the most

widespread and commonly asked security questions are still drawn from Haga and Zviran's list. In part this is due to the fact that many websites do not write their own security questions. Instead, their authentication protocols are implemented by outside contractors, like the multinational corporation RSA Security LLC. As a result, a common pool of security questions are used across a wide variety of sites. Yet what becomes clear in tracing these questions back to Haga and Zviran's study, which included no discussion of how the researchers arrived at the questions they recommended, is that the specific semantic and social content of security questions has rarely been explored, even by the researchers who study them.

Though they are as old as the issue of authenticating web-based data itself, security questions did not enter their heyday until the early 2000s, when it became increasingly common to incorporate questions about users' personal information into individual online account management. By approximately 2007, security questions had hit peak adoption. They were used by financial institutions, credit card companies, utilities companies, government agencies, and email service providers, to name just a few sectors in which they became key fixtures of managing identity and access. The ubiquity of these questions was sufficiently notable to inspire one cultural commentator to publicly bemoan what he saw as the "impossible to answer, frequently creepy, and rarely secure" questions that seemed "suddenly omnipresent" online.¹⁶ To be a digital subject in the moment that this observer is describing, amid an online environment structured through accounts and log-ins, meant facing iterations of these questions on a regular basis. Authenticating oneself by determining and recalling the correct responses to personal questions was now a nearly unavoidable piece of the experience of personhood on the Internet. Only a few years later, starting in approximately 2011, a number of large companies, including Facebook and Google, began phasing out security questions from their authentication protocols—though others, like Apple, continue to use them (fig. 1). Today, the latest wave of studies on security questions recommends against their use, arguing that answers are in fact easier to guess and harder to remember than previously supposed.¹⁷

Security questions may have passed their peak in popularity, but the same cultural forces that act through security questions continue to shape the experience of digital subjecthood in crucial ways. Facebook's "real name" policy, for example, demonstrates that the "severe problem of authenticity," as it was called in 1987, is still a central concern—both for those who seek to verify the identities of their users and for those who seek to live their lives in digital spaces

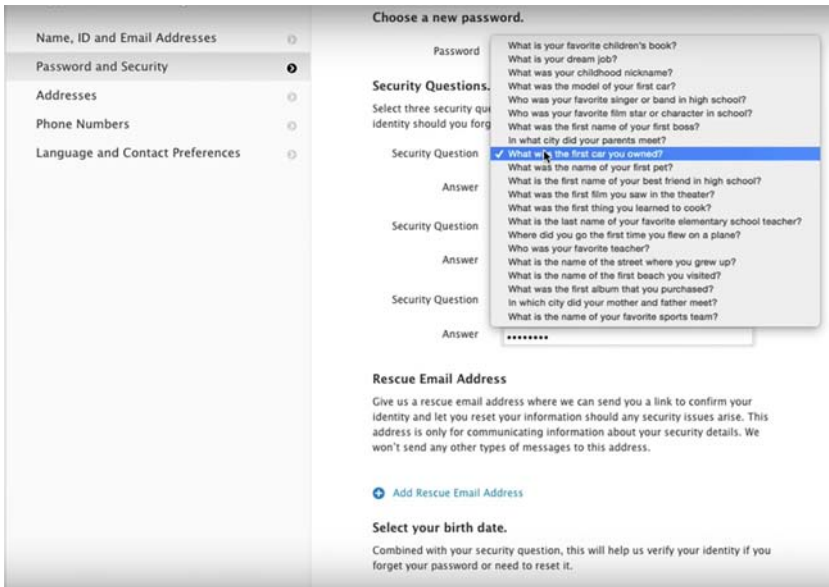


FIGURE 1. A screenshot from Apple's password recovery page in 2015, including a drop-down list of security questions, many of which relate to romantic relationships or family ties.

without needing to contort themselves (for instance, by inventing false responses that overwrite their own lived experiences) in order to produce answers that satisfy the rigid and biased presumptions of data.

AUTHENTICATING IDENTITY THROUGH HETERONORMATIVITY

Along with the online security question has come an underlying set of problematic assumptions about what kinds of data should be used to establish legitimate subjecthood in digital spaces. With notable frequency, the security questions that have been most widely implemented on the Internet require users to produce answers that comply with dominant expectations for femininity, masculinity, romance, reproductivity, and family relationships. Notably absent from published work on security questions is a meaningful critique of the semantic content of these questions: not just how they function as regulating protocols, but what they actually say. The exclusive focus on the effectiveness of security questions to regulate access to databases (in the contemporary context) has left little room for reflection on the cultural logics that structure authentication itself.

Why does the rhetorical content of online security questions matter? The answer lies in the way that these questions codify and impose a system of beliefs about identity itself. In effect, security questions can be understood as tools used to determine whether a user is “real” in a conceptual as well as a pragmatic sense. That is, when a person passes the test of authenticity, they are deemed to be “really” themselves and given access to their account. Conversely, failing the test of authenticity means failing to convincingly *be* oneself—being revealed as a fake or a “pretender”—and therefore being denied access. Fundamentally, then, online security questions set the terms of what it means to be a legitimate subject. Security questions do this cultural work by filtering users through mainstream expectations about normalcy and problematic presumptions of universality. They present themselves as so broadly relevant that any user will have an answer to them. Critics of security questions have bemoaned the fact that answers to some of these questions (for example, “What is your favorite flavor of ice cream?”) are bound to change, making them difficult to recall. Yet far more insidious is the underlying suggestion that these questions, as worded, should apply to every authentic subject. Users for whom the very premise of the question is not applicable become suspect precisely because their identities, experiences, or desires do not fit culturally constructed standards for what types of personal data qualify a subject for basic selfhood.

The hegemonic policing of identity that online security questions perform is most apparent in the prevalence of heteronormativity in these questions. A survey of frequently used online security questions confirms that a striking percentage directly relate to normative expectations regarding romantic relationships and reproductivity.¹⁸ These questions are structured around the presumption that users share what is imagined as the universal experience of heterosexual partnership—a partnership that follows dominant cultural narratives about courtship, marriage, and the formation of family. The following questions, pulled from online account authentication systems currently or previously in use by a representative selection of top companies and organizations, exemplify this trend:

In what city did you meet your spouse? (AT&T, Vanguard)

In what city were you married? (Vanguard)

Where did you go on your honeymoon? (Comcast, Yahoo)

What is the first name of the best man / maid of honor at your wedding?

(Yahoo, California Department of Motor Vehicles)

What is the name of the medical professional who delivered your first child?

(California Department of Motor Vehicles)

What is your youngest child's nickname? (Yahoo)¹⁹

It is striking how many of these questions proceed from the assumption that the user is married and, secondarily, has children. They reflect a belief system in which the “authentic” subject is a straight subject—or alternatively, to use the term popularized by Lisa Duggan, a homonormative one.²⁰ The questions “In what city did you meet your spouse?” and “In what city were you married?” for example, proceed from the presumption that the user not only is or has been married, but that they have reliable, safe, legal access to marriage, a privilege that has been denied to many LGBTQ people in America throughout the security question’s online history. Questions such as “What is the first name of the best man / maid of honor at your wedding?” and “Where did you go on your honeymoon?” additionally presume that the user’s marriage has followed mainstream wedding traditions, often undertaken at considerable expense. Meanwhile, “What is your youngest child’s nickname?” implies that a standard user will have not one but multiple children—and the question regarding medical professionals assumes that a user will have biological rather than adopted children, as is the case for many LGBTQ parents. Often, online account setup systems that use security questions do allow users to choose which questions they answer. However, heteronormative questions like these are so prevalent that it can be difficult to complete the sign-up process without being required to answer at least one.

Other widely used online security questions are less explicit in their heteronormative assumptions. Nonetheless, these questions too are founded on hegemonic beliefs about romantic relationships, value, and identity:

What is the first name of the boy or girl that you first kissed? (Southern California Edison)

What was the first name of your first girlfriend or boyfriend? (Vanguard)

At first glance, these questions may appear less problematic than those in the first group. Apart from their perpetuation of the notion of binary gender, they seem to accommodate LGBTQ users, who are not restricted in selecting between a girlfriend or a boyfriend. What makes these questions heteronormative relates to the concept of “non-triviality.” Online security questions are designed to have memorable answers—answers that users will remember over the life of their account access. In this sense, they are based on beliefs about what elements of their lives the user should value. The presumption that one’s first kiss or first partner is fundamentally valuable to one’s identity, and valuable in perpetuity, reflects a cultural narrative about romance that does not account for the experiences of those whose sexual identities or personal histories (such as histories of sexual abuse) may

fundamentally shift the meaning that they make from these early romantic experiences.

Similar in the ways that they enact heteronormative systems of value are questions about users' childhoods and families of origin, such as:

What is the first name of your favorite uncle? (Yahoo)

What was the name of your favorite elementary school teacher? (Wordpress, Apple, Yahoo)

Questions of this sort, asking for the names of favorite relatives or beloved figures from one's youth, are among the most widely used by online authentication systems. Such questions may appear, at first, indeed universal. The key point of critique here, however, is in the word "favorite." A positive relationship with one's biological family and a sense of nostalgia for one's childhood are themselves privileges more commonly afforded to straight, cisgender subjects than to queer ones, or to others in marginalized subject positions, such as people with disabilities or non-neurotypical people, for whom the challenging interpersonal dynamics encountered in childhood may have been ones to survive rather than to cherish. These questions presume not only that the user had a favorite uncle or elementary school teacher, but that family and childhood memories should be fundamentally and permanently valued by the user.

And no accounting of heteronormative online security questions would be complete without considering that most canonical of questions: "What is your mother's maiden name?" Today, "mother's maiden name" primarily appears in security research as an illustration of the type of question that is no longer effectively secure in the digital age because of increased access to public records and social media.²¹ However, the "mother's maiden name" question still appears in selected online contexts—and in popular discussions around authentication it continues to function as shorthand for the security question itself.²² Fittingly, "What is your mother's maiden name?" also exemplifies the heteronormative assumptions of the sort that structure so many online security questions. This one question alone presumes:

1. that the respondent's parents were married;
2. that therefore, given the history of marriage laws both in America and internationally, the respondent's parents were likely straight;
3. that the respondent was not born to or adopted by a single parent, but was a member of a normative family unit;
4. that the respondent's mother took her husband's last name after marriage.

The “mother’s maiden name” question presents itself as requesting a simple, objective piece of personal data. Yet deconstructing the question in this way exposes the extent to which it in fact proceeds from multiple points of cultural bias—and, more specifically, biases related to gender roles for women. Those for whom the above assumptions are not true must lie to render themselves authentic subjects—subjects who can be authenticated. A respondent whose mother was married but who did not change her last name, for example, must override the politics of their mother’s own decision regarding her name and accept the premise of the question in order to answer it, give proof of identity, and gain access to basic online services. Having an answer to this question, or at least being willing to *pretend* to have one, becomes a basic requirement for personhood—in this and all security questions.

SECURITY QUESTIONS: A PRE-DIGITAL HISTORY

In order to understand how the logics of heteronormative personhood have come to shape the rhetoric of online security questions, as well as broader notions of identity and authenticity in digital spaces, we must turn from the twenty-first century to the nineteenth and trace the history of these questions back to their pre-digital roots. The origins of the security question in fact date to a moment long before the widespread adoption of the desktop terminal or the rise of the World Wide Web, before the invention of any data management technology that might today be called “digital”—to the year 1850. Although the security question took on new life at the turn of the twenty-first-century, the tumultuous scene of its birth was not the transition to personal computing that has marked recent decades, but another moment of profound cultural change: the rapid growth of the northeastern cities in mid-nineteenth-century America—and the questions, challenges, and changes around identity, citizenship, and authenticity brought on by that growth.

In many ways, the story of the security question is a story of the American bank. Online banking was among the first sectors to embrace and pervasively implement security questions as protocols for protecting against unauthorized account access. In 2005, a report on “Authentication in an Internet Banking Environment” from the Federal Financial Institutions Examination Council strongly encouraged all banks to use “shared secrets” in addition to passwords.²³ By 2008, it has been estimated that 90 percent of American banks had incorporated security questions into their online account management systems.²⁴ Today, even as the popularity of security questions declines, they are still nearly ubiquitous on websites associated with the management of users’ personal

finances. It is perhaps unsurprising then that the security question was invented and popularized by banks. When researchers on the security of information systems began outlining authentication protocols in the 1970s and 1980s, it was standard banking practices that inspired the guidelines they prescribed.²⁵ Many of the functional and cultural logics that structure online security questions can be traced back to these banking practices and the historical and cultural contexts of their emergence.

The security question itself, or what was initially called the “test question,” was invented by the Emigrant Industrial Savings Bank in New York and first implemented in 1850. Emigrant was established to serve Irish immigrants who had fled the potato famine and were arriving in New York at the unprecedented rate of approximately twenty-five thousand each year.²⁶ In America, the Irish faced discrimination from xenophobic, anti-immigrant “nativists” and often found themselves unwelcome in mainstream financial institutions, and were therefore more vulnerable to banking fraud. Founded by the Irish Emigrant Society in conjunction with the Roman Catholic archdiocese, Emigrant was imagined as a resource for members of the Irish American community to safely store their savings and send money back to family members in Ireland.²⁷

At the time, the standard procedure for managing withdrawals from an individual account in American banks was the use of a “signature book” or passbook. Account holders were required to present the book and sign an entry when withdrawing money in order to prove their identities. Many of Emigrant’s clients were illiterate, however, and so the signature book was replaced with a new system for identity verification: the test book (fig. 2). These test books—according to the historian Richard Salvato, who prepared thirty-five volumes of Emigrant’s documentation dated from 1850 to 1880 for entry into the New York Public Library archives in 1997—“contain an extraordinary abundance of detailed personal and family information” which was used “as a practical identity test.”²⁸ When setting up new accounts, clients were asked questions regarding their birthplace, their arrival in America, and their family members. This information was then used to verbally quiz account holders, allowing Emigrant to authenticate clients in a way not previously seen in American banking.

It took approximately fifty years for the mainstream American banking sector to begin its widespread adoption of security questions. Discussions of the merits and applications of the security question started making regular appearances in the leading industry journal of the day, *Bankers’ Magazine*, in 1904, with a survey of existing methods for authenticating access to safe deposit boxes.

| DATE | NUMBER | SIGNATURE | RESIDENCE | OCCUPATION | WHERE BORN | RELATIONS |
|----------|--------|----------------------------------|-----------|------------|------------|---------------|
| 1870 | | | | | | |
| March 28 | 1897 | Mary G. G. | 119 | Teacher | 1324 | of Mary G. G. |
| June 29 | 200 | Mary & Elizabeth Mary & James | 119 | Teacher | 1324 | of Mary G. G. |
| | 201 | Mary & Elizabeth | 119 | Teacher | 1324 | of Mary G. G. |
| | 210 | Mary & Elizabeth | 119 | Teacher | 1324 | of Mary G. G. |
| | 223 | Mary & Elizabeth | 119 | Teacher | 1324 | of Mary G. G. |
| | 239 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 253 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 264 | John & Elizabeth | 119 | Teacher | 1324 | of Mary G. G. |
| | 287 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 298 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 307 | Thomas O. Brown | 119 | Teacher | 1324 | of Mary G. G. |
| | 343 | A. Lee Kelley | 119 | Teacher | 1324 | of Mary G. G. |
| | 345 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 357 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 362 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 364 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 365 | | 119 | Teacher | 1324 | of Mary G. G. |
| | 369 | Thomas & Elizabeth | 119 | Teacher | 1324 | of Mary G. G. |

FIGURE 2. A page from an Emigrant Industrial Savings Bank test book with entries recorded in 1870. Note the “relations” column on the right, which includes maiden names.

Though some banks relied on physical appearance to verify box holders’ identities, requiring that tellers know their clients by sight, the authors of the report recommended recording “certain fixed data in regard to a renter” on which those laying claim to the box could later be tested, “as this will be a help in establishing more surely [their] identity” and ensure that only “reasonable and desirable persons” engaged in business with the bank.²⁹ This sentiment, as well as the rhetoric of the “desirable” person, is echoed in a 1906 article in which the author urges fellow bankers to use the collection of personal data to ensure that the would-be box holder is a “person of ordinary honesty.”³⁰

In the same year, William H. Hayden published an article titled “System in Savings Banks” in *Bankers’ Magazine* that serves as a key document for tracing the pre-digital history of the security question. Hayden describes how in 1889 his own bank, the Eutaw Savings Bank of Baltimore, began restructuring its functional operations according to that of the “excellent Emigrant Industrial Savings Bank.” Fundamental to this system was the keeping of “record cards.” Like Emigrant’s test book entries, these cards

recorded personal information and functioned as proto-profiles. Whereas signatures could be forged, argued Hayden, the record cards facilitated “a strong test of identity.”³¹ In the decades that followed, Emigrant’s security question protocols, popularized through Hayden, came into use throughout the country. From their origins at Emigrant Industrial Savings Bank, through their adoption at the Eutaw Savings Bank, these questions entered widespread use in contexts far beyond the specific cultural and political pressures that inspired their original implementation.³²

The pre-digital history of what would later become the online security question demonstrates how issues of authenticity and realness, as well as experiences of discrimination, have been central to the development of identity verification protocols for more than a century and a half. Developed in response to the specific obstacles faced by Irish immigrants, the security question can be understood as a technology specifically designed to both accommodate and regulate a marginalized portion of the population. In this sense, the anxiety that drives the push to identify “reasonable and desirable persons” (versus the “pretender”) is fundamentally linked to anxieties around immigration, cultural shift, and the implicit threat of the “undesirable” subject. The challenges of poverty, unequal access to education, and reactionary xenophobia sparked the initial innovation of the security question. Yet this spark grew, in time, into a set of widely adopted, institutionalized, and normativized expectations for verifying identity itself, not just the identity of members of one specific group. However, even when the implementation of the protocol became pervasive, extending far beyond the Emigrant Industrial Bank and communities of Irish immigrants, this historical context and its social implications lived on within the foundations of the security question protocol.

WHAT IS YOUR MOTHER’S MAIDEN NAME?

The heteronormativity that characterizes many contemporary online security questions in fact has its roots in the security question’s pre-digital history. This can be seen specifically through the example of the question “What is your mother’s maiden name?” It is not coincidental that the “mother’s maiden name” question has become the best known of security questions. This is because it is not just a common security question; it is actually the *original* security question. Indeed, this question was born in the same instant as the technology of the question-and-answer protocol itself. Therefore, it demonstrates how the place of normative assumptions about gender and sexuality are more than an incidental by-product of security questions in their modern-day format. To the

contrary, heteronormativity shaped the logics behind security questions' very beginnings. Looking at the documentation that surrounds the history of the security question reveals that the "mother's maiden name" question can be traced from Emigrant's test books, through each step of the shifting bank protocols of identity verification, into the formative research that brings security questions to the digital realm, and finally in present-day standards. For this reason, the "mother's maiden name" question demonstrates how issues of gender and sexuality are central to the history of the security question. Because the question appears time and again in the materials that tell the story of the security question over the last one hundred and fifty years, it is clear that "What is your mother's maiden name?" has been an ongoing benchmark that continues to contribute to both the forms and the functions of identity verification structures.

The first recorded instance in which the "mother's maiden name" question was used as an identity verification protocol comes from none other than the Emigrant Industrial Savings Bank. Among the personal data collected in Emigrant's test books for quizzing clients was a range of information regarding family members. An example entry from the early days of Emigrant's test book accounting looks like this:

Date deposit-account opened: 1856, Oct 18. Deposit account number: 2987.
Name: Michael Sullivan. Occupation: farmer. Residence: New Lots, L. I.
Remarks: Native of Kilmackrahan, 5 miles from Kamturk, County Cork, Ireland. Arrived in New York July 19, 1851 on the *Radiana* via Cork from Liverpool. Family in Ireland, father Cornelius, mother Ellen Dial, dead, two brothers in Ireland, Cornelius and David. One sister, Ellen, is dead. Is single.³³

Of note here, first, is that the type of data considered valuable for verifying identity, along with information regarding one's place of birth and journey to America, is primarily data regarding one's family and marital status. This reflects an early emphasis on authenticating selfhood through data points related to family structures, which we see continued in contemporary security questions. More to the point, though, it is telling to observe that all family members recorded in this account holder's test book entry are listed using only first names—except for the account holder's mother, who is listed as "Ellen Dial" (Dial being presumably her maiden name). Here we are seeing an answer given to the "mother's maiden name" question as it was posed to the account holder by the clerk who made this entry in the test book at Emigrant.

Why should this first recorded incarnation of the "mother's maiden name" question appear here specifically, in Emigrant's test books? In the absence of

primary writing on the subject from the architects of Emigrant's identity verification protocols, the bank's intentions are uncertain, but informed speculation opens up a number of suggestive possibilities. One potential answer is that the question itself was fundamentally linked to the experience of Irish immigrants in mid-nineteenth-century America, for whom the bank's systems were explicitly tailored. On the one hand, the additional layer of security represented by needing to list one's family members, and moreover to provide a maiden name for one's mother, could be seen as a manifestation of anti-immigrant sentiment. Asking for a mother's maiden name provides an additional piece of information to verify identity, suggesting an implied concern that immigrants may be less trustworthy and more likely to misrepresent themselves. This question could also potentially serve as a tool for determining family legitimacy—that is, determining whether an immigrant's parents were married or whether the potential account holder was (to use a term that resonates with the rhetoric of authentication) "illegitimate." Whatever the question's intended purpose, it is certain that Emigrant's test book protocols emerged at a moment of cultural anxiety around immigration. The increased level of scrutiny that the test books represented suggests that the security question may have been born out of a biased sense that US citizens could be trusted to represent themselves truthfully, whereas immigrants needed to be thoroughly quizzed to prove their identities.

Yet it is important to remember that Emigrant was established by members of the existing Irish American community in New York, and therefore was likely operating under less xenophobic beliefs about the legitimacy of immigrant subjects. In this sense, we might say that the Emigrant test books represent the documentation of immigrant identities from within the Irish American community. Consider, by contrast, the types of identity documentation performed by systems created outside the Irish American community—for instance the records kept at Castle Garden in the Bowery, the precursor to Ellis Island. While these records also list information regarding an immigrant's voyage to America, they record considerably less data about family members and, importantly, do not include information about mothers' maiden names.³⁴ Perhaps then we can understand the attention to family history in Emigrant's test books as a reflection of shared Irish and Irish American cultural values, such as an emphasis on family lineage that could be used to trace one's roots back to relatives in Ireland. Alternatively, the inclusion of a mother's maiden name might be seen as a gesture through which Irish Americans, facing discrimination by mainstream society, attempted to legitimize new members of their community through the establishment of normative family structures.

When the security question began to spread to banks across America in the 1890s and 1900s, the “mother’s maiden name” question spread with it. Variations on this question are the most consistently cited example of the question-and-answer format given by banking professionals in contemporaneous writings on security protocols. In fact, it is in this shift into mainstream banking usage that the “mother’s maiden name” question goes from being one particularly notable question among a number of questions (as was the case in Emigrant’s system) to being the quintessential security question—the one called out most explicitly and most often. Hayden, in the same report in which he popularized elements of Emigrant’s test book system, calls the “mother’s maiden name” question the “strongest test of identity.”³⁵ Reports in *Bankers’ Magazine* on the security protocols of safety deposit boxes from 1904 and 1906 explicitly underscore the value of the “mother’s maiden name” question. “It is well,” writes one bank manager, “to secure certain fixed data in regard to a renter, such as when born, your father’s name and mother’s maiden name.”³⁶ Information of this sort, the report goes on, is particularly useful for verifying identity because it is more reliable than using password systems, since passwords are “easily forgotten and of doubtful utility”—a phrase that could have been taken directly from modern-day writing on the advantages and disadvantages of different cybersecurity protocols.³⁷ It is also worth lingering on the phrase “fixed data.” Such rhetoric clearly signposts the beginnings of a shift away from older ways of conceptualizing identity and security toward a model that presciently echoes the contemporary spirit of big data.

Once the security question had become common practice in banking, the “mother’s maiden name” question—and the association of heteronormative questions of this sort with reliable identity verification—was nearly ubiquitous. A 1912 survey of the paperwork used for account withdrawals by a variety of major US banks demonstrates that, while security question practices varied somewhat, all of the institutions surveyed asked for mothers’ maiden names.³⁸ It is also around this time that the more free-form entry from the Emigrant test book transformed into a more rigid set of ledgers and forms with standardized questions and response area boxes: strongly visually recalling the modern online user profile.³⁹ These documents also show that the broad interest in family data found in Emigrant’s test books had narrowed to focus almost entirely on one piece of information: the mother’s maiden name. Whereas Emigrant’s early test books recorded the names of siblings, aunts, both parents, et cetera, creating a richer picture of lineage and interpersonal connections, the security question protocols that were becoming increasingly standardized asked only for the

mother's maiden name. In fact, this is even true of Emigrant Industrial Savings Bank, which by the 1910s had updated its security protocols to keep up with the times and now used a standardized account withdrawal slip with a designated area for answering the "mother's maiden name" question (fig. 3). In the decades since the first use of the security question, its heteronormative logics had been increasingly distilled and reinforced, until the question that alone seemed satisfactory to determine the authenticity of one's identity was, "What is your mother's maiden name?"

Driving the increased adoption of the security question was a sense of concern that the day-to-day operations of banking were becoming less secure and that verifying identity was becoming increasingly difficult. Much of the professional writing from bankers at this time demonstrates a rising anxiety around the sense that existing methods of authentication were proving insufficient. In particular, this writing belies a newly emergent yet marked distrust in the body as a site of reliable authentication. Among the long-standing protocols most often critiqued by bankers in the 1900s and 1910s are those that rely on the bank employee to recognize some part of the account holder's physical presentation. Using the account holder's signature (or handwriting) or personal appearance to verify identity came particularly under fire. In 1906, Clay Herrick warned his fellow bankers that identifying account holders by height, complexion, and "visible scars or marked peculiarities" can lead to confusion as customers age. "Of more value," he says, "are such facts as the date and place of birth, father's name and mother's maiden name."⁴⁰ In 1904, A. J. Enright et al. wrote of bank account management procedures: "Some companies . . . require that a record be kept of physical appearance. . . . This, however, is not an essential, as it is to be presumed that the renter will remain a customer for a number of years, during which time physical conditions may change." Enright recommended instead that banks use information like an account holder's mother's maiden name to verify identity, since this information is "fixed and cannot change, and [is], therefore, as reliable twenty years hence as to-day."⁴¹ Here we see illustrated a fundamental shift in concepts of knowability. The body is perceived as "insecure," not necessarily because it can be forged or faked, but because it can change. "Fixed data" such as an account holder's mother's maiden name, by contrast, is regarded as trustworthy specifically because it is perceived as immutable.

However, the very same traits that are imagined to make these points of "fixed data" particularly trustworthy are also those that make heteronormative security questions so oppressive. On the surface, these bankers' reports give voice to a goal that continues to be echoed in writing on digital security

**EMIGRANT INDUSTRIAL SAVINGS
BANK,**

51 Chambers Street, New York.

**REQUIRED OF DEPOSITORS ON
OPENING ACCOUNTS:**

| | | |
|---|---|---|
| Sign your name twice. First name in full. | } | It is agreed, that this account shall be subject to the By-Laws of the Emigrant Industrial Savings Bank. |
| | | It is agreed, that this account shall be subject to the By-Laws of the Emigrant Industrial Savings Bank. |
| Address, | | |
| Occupation, | | |
| Date of Birth, | | |
| Where Born, | | |
| Give the city or town and the country or State. | | |
| If Born Abroad, Date of Arrival in America | | |
| Per Ship, | | |
| Give the Full Name of Each. | } | Father, |
| | | Husband, |
| | | Wife, |
| | | Before her marriage. |
| | | Mother, |
| | | Before her marriage. |

TAKE NOTICE.—The Pass Book is the voucher for payment; therefore, keep it in some place safe and secure from loss or theft.

No Draft will be paid, unless the signature of the depositor is recorded with the Bank; in case he cannot write, his mark must be acknowledged before a Notary Public, with a notarial seal, and the acknowledgment attached to the draft.

No Draft or Deposit made without the production of the Pass Book.

FORM 1.—FOR OPENING ACCOUNTS

FIGURE 3. A form for opening a new account at Emigrant Industrial Savings Bank in 1912, which includes a space for one's mother's name "before her marriage."

protocols today: the search for those pieces of data that will most effectively restrict account access to authorized users. Yet let us linger here to ask *why* the answer to the "mother's maiden name" question was seen as particularly secure. The three explanations that appear throughout these reports are: that a mother's maiden name will not change, that it will be memorable to the account holder, and that it will be so obscure as to be, in Hayden's terms, "rarely known"

even by those who know the account holder's family well.⁴² Indeed, these qualities are still the measures by which database security experts describe a strong password or security question answer. But to characterize a mother's maiden name, as a unit of information, according to these guidelines is fundamentally sexist. It inscribes onto the maiden name the work of upholding heteronormativity in order to ensure the fixedness required for the reliable verification of identity.

Setting aside for the moment the problematic presumption that a mother's maiden name is universally memorable, or that all "desirable persons" know their mothers, or even that a respectable person (that is, the desired type of person opening a bank account) must have a mother who is married, the basic implication that a mother's maiden name is "rarely known" is highly problematic. Across the history of the security question, identity verification protocols have foregrounded this particular question not because the mother's maiden name is seen as so important, but because it is seen as uniquely unimportant. That is, a woman's maiden name (and by extension her life before and outside of heterosexual marriage) is considered so obscure a piece of trivia that no would-be perpetrator of bank fraud could know it. In this way, the central place of the "mother's maiden name" question in the history of digital account management demonstrates how identity verification functions at even the most basic of levels around discriminatory logics that demand feminist critique.

GENDER AND DIGITAL SUBJECTHOOD

As this history of the security question has demonstrated, notions of authentic selfhood in digital spaces today are inextricably bound up with normative expectations of gender, sexuality, and identity. Tracing this history has shown that the reason that contemporary security questions continue to be so heteronormative in their structuring logics is that the security question that has shaped the protocol for more than a hundred and fifty years ("What is your mother's maiden name?") is itself founded on sexist logics that have become inseparable from the protocol of the security question itself. At the same time, looking at the history of "mother's maiden name" speaks to a moment of cultural shift and anxiety around identity and subjecthood that resonates in many ways with the present moment. The security question emerged from a moment of change around perceptions of citizenship and authentic personhood with parallels to contemporary issues around digital citizenship. In this way, the history of online security questions suggests

that heteronormative logics may serve as fallback for attempting to structure and thereby control knowledge at times of cultural change.

The history of the security question also serves as a window onto a larger set of issues around selfhood, identity, and knowability as they relate to data. If the birth of the security question marks a foundational point on the path to the contemporary ethos of “objective” big data, it is telling that that foundation is rooted in heteronormative assumptions about the lives and values of “authentic” personhood. Ultimately, this work demonstrates how the histories of digital protocols, traced to a pre-technological moment, can reveal the cultural biases and social pressures that have shaped those protocols. Far from being objective tools, these tools also perpetuate the biases and cultural implications they carry forward from their histories. ■

BONNIE RUBERG is a postdoctoral scholar in the Interactive Media and Games Division at the University of Southern California and an assistant professor of informatics at the University of California, Irvine. They received their PhD from the University of California, Berkeley, with emphases in new media and gender studies. Their research focuses on gender and sexuality in digital media. They are the coeditor of the volume *Queer Game Studies* (University of Minnesota Press, 2017) and the lead organizer of the annual Queerness and Games Conference. Previously they have worked as a technology journalist for the *Village Voice* and other publications.

NOTES

1. Lisa Gitelman, ed., *“Raw Data” Is an Oxymoron* (Cambridge, MA: MIT Press, 2013), 3.

2. See Mike Just, “Designing and Evaluating Challenge-Question Systems,” in *Proceedings of the IEEE Computer Society* (2004), <http://homepages.inf.ed.ac.uk/mjust/papers/JustIEEEPaper.pdf>.

3. Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson, “Secrets, Lies, and Account Recovery: Lessons from the Use of Personal Knowledge Questions at Google,” proceedings of the 24th International World Wide Web Conference (2015), 141–50, <http://delivery.acm.org/10.1145/2750000/2741691/p141-bonneau.pdf>.

4. See Theodore M. Porter, *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life* (Princeton, NJ: Princeton University Press, 1995), 3.

5. See Daniel Rosenberg, “Data before the Fact,” in *“Raw Data” Is an Oxymoron*, 15–40.

6. Wendy Hui Kyong Chun, *Control and Freedom: Power and Paranoia in the Age of Fiber Optics* (Cambridge, MA: MIT Press, 2006); N. Katherine Hayles, *My Mother Was a Computer: Digital Subjects and Literary Texts* (Chicago: University of Chicago Press, 2005); Lisa Nakamura, *Cybertypes: Race, Ethnicity, and Identity on the Internet* (New York: Routledge, 2002).

7. Craig Robertson, *The Passport in America: The History of a Document* (New York: Oxford University Press, 2010), 3.

8. Craig Robertson, "A Documentary Regime of Verification," *Cultural Studies* 23, no. 3 (2009): 329.

9. Rena Bivens, "The Gender Binary Will Not Be Deprogrammed: Ten Years of Coding Gender on Facebook," *New Media and Society*, December 27, 2015, <http://journals.sagepub.com/doi/full/10.1177/1461444815621527>.

10. Amanda Holpuch, "Facebook Still Suspending Native Americans Over 'Real-Name' Policy," *TheGuardian.com*, February 16, 2015, accessed September 28, 2016, <https://www.theguardian.com/technology/2015/feb/16/facebook-real-name-policy-suspends-native-americans>; Amanda Holpuch, "Facebook under Fire from Drag Queens over 'Real-Name' Rule," *TheGuardian.com*, September 13, 2014, accessed September 28, 2016, <https://www.theguardian.com/technology/2014/sep/13/facebook-under-fire-drag-queens-real-name-rule>.

11. Elizabeth Freeman, "Queer Belongings: Kinship Theory and Queer Theory," in *A Companion to Lesbian, Gay, Bisexual, Transgender, and Queer Studies*, ed. George E. Haggarty and Molly McGarry (Oxford: Blackwell, 2007), 295–314; Jack Halberstam, *In a Queer Time and Place: Transgender Bodies, Subcultural Lives* (New York: New York University Press, 2005).

12. See Porter, *Trust in Numbers*, vii.

13. Niv Ahituv, Yeheskel Lapid, and Seev Neumann, "Verifying the Authentication of an Information System User," *Computers and Security* 6 (1987): 152, my emphasis.

14. *Ibid.*, 153.

15. William J. Haga and Moshe Zviran, "Question-and-Answer Passwords: An Empirical Evaluation," *Information Systems* 16, no. 3 (1991): 335–43.

16. Josh Levin, "In What City Did You Honeymoon? And Other Monstrously Stupid Bank Security Questions," *Slate*, January 29, 2008, accessed September 20, 2016, http://www.slate.com/articles/technology/technology/2008/01/in_what_city_did_you_honeymoon.html.

17. See Bonneau et al., "Secrets, Lies, and Account Recovery," 141–50; Ariel Rabkin, "Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook," proceedings of the 4th Symposium of Usable Privacy and Security (2008), 12–23, <https://cups.cs.cmu.edu/soups/2008/proceedings/p13Rabkin.pdf>; Jack Lindamood, Raymond Heatherly, Murat Kantarcioglu, and Bhavani Thuraisingham, "Inferring Private Information Using Social Network Data," proceedings of the 18th International World Wide Web Conference (2009), 1145–46, <http://www.utdallas.edu/~muratk/publications/www09pp242-lindamood.pdf>.

18. See Abrah Ullah, Hannah Xiao, Mariana Lilley, and Trevor Barker, "Privacy and Usability of Image and Text Based Challenge Questions Authentication in Online Examination," proceedings of the 2014 International Conference on Education Technologies and Computers (2014), 24–29, <http://ieeexplore.ieee.org/document/6998897/>.

19. Here I have tried to represent a diversity of the types of institutions with notable web presences that use (or up until recently have used) security questions in their

verification protocols. I collected some of these questions from websites that I myself use; others I gleaned from YouTube videos uploaded by users documenting website sign-up processes.

20. Lisa Duggan, *The Twilight of Equality?: Neoliberalism, Cultural Politics, and the Attack on Democracy* (Boston: Beacon, 2003).

21. See Virgil Griffith and Markus Jakobsson, "Messin' with Texas: Deriving Mother's Maiden Names Using Public Records," proceedings of the Third International Conference on Applied Cryptography and Network Security (2005), 91–103, <http://www.romanpoet.org/1/mmn.WithFiguresFinal.pdf>; Rabkin, "Personal Knowledge Questions for Fallback Authentication."

22. See Kasmir Hill, "Your Mother's Maiden Name Has Been a 'Security Question' since 1882," Fusion.net, March 12, 2015, accessed September 22, 2016, <http://fusion.net/story/62076/mothers-maiden-name-security-question/>.

23. Federal Financial Institutions Examination Council, "Authentication in an Internet Banking Environment" (2005), https://www.ffiec.gov/pdf/authentication_guidance.pdf.

24. Levin, "In What City Did You Honeymoon?"

25. See Dennis K. Branstad and Miles E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers and Security* 1 (1982): 255–60.

26. See Marion R. Casey, "Refractive History: Memory and the Founders of the Emigrant Savings Bank," in *Making the Irish American: History and Heritage of the Irish in the United States*, ed. J. J. Lee and Marion R. Casey (New York: New York University Press, 2007), 306.

27. Richard Salvato, "A User's Guide to the Emigrant Savings Bank Records," New York Public Library Manuscripts and Archives Division (1997), 2, http://archives.nypl.org/uploads/documents/other_finding_aid/collection_1837_emigrant.pdf.

28. *Ibid.*, 4.

29. A. J. Enright, S. F. Haserot, E. Shorrock, and Clark Williams, "Report of Special Committee on the Classification of Legal Decisions Relating to Safe Deposit Companies," *Bankers' Magazine* 69, no. 4 (1904): 587.

30. Clay Herrick, "Trust Companies: Their Organization, Growth and Management," *Bankers' Magazine* 72, no. 3 (1906): 419.

31. William H. Hayden, "System in Savings Banks," *Bankers' Magazine* 73, no. 5 (1906): 765, 767.

32. See M. F. Bauer, "The Tellers of a Commercial Bank," *Bankers' Magazine* 85, no. 2 (1912): 137–41; "Payments upon Forged Orders," *Bankers' Magazine* 88, no. 5 (1914): 581–82; William H. Kniffin, "Savings Departments in Banks of Discount and Trust Companies," *Bankers' Magazine* 106, no. 3 (1923): 468–73; Glenn G. Munn, "Savings Banking," *Bankers' Magazine* 110, no. 3 (1925): 531–35.

33. Salvato, "A User's Guide to the Emigrant Savings Bank Records," 4.

34. The archives of the Ellis Island Foundation Inc., libertyellisfoundation.org.

35. Hayden, "System in Savings Banks," 767.

36. Enright et al., "Report of Special Committee on the Classification of Legal Decisions Relating to Safe Deposit Companies," 587.

37. Herrick, "Trust Companies," 420.
38. Bauer, "The Tellers of a Commercial Bank," 140.
39. Ibid., 138.
40. Herrick, "Trust Companies," 419.
41. Enright et al., "Report of Special Committee on the Classification of Legal Decisions Relating to Safe Deposit Companies," 587.
42. Hayden, "System in Savings Banks," 768.